PC WELT SONDERHEFT
Juni/Juli/August 2006
www.tecChannel.de

200 Seiten Profi-Wissen

tecCHANNEL

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 10,90
Österreich € 12,00
Benelux € 12,55
Schweiz SFR 21,80

Unentbehrliches Netzwerk Know-how

- Grundlagen aus der Cisco Networking Academy
- Wissen: VLANs, Routing und Subnetze
- Praxis: LDAP & Nameserver richtig konfigurieren

Sicherheit für Desktops und Server

- Hilfe: Katastrophenszenarien bei Active Directory
- Wissen: Zugriffskontrolle bei Samba 3
- Praxis: Linux härten

4 195914 910906 03

Editorial

„Der Strom kommt aus der Steckdose“

So wenig wie viele über die Elektrizität nachdenken, so wenig denken sie auch über das Netzwerk nach. Dass sie in einem Netzwerk arbeiten, wird den meisten Nutzern erst bewusst, wenn ein Fehler auftritt. Kein Wunder, passiert die meiste Arbeit doch unbemerkt in anderen Bereichen des Unternehmens. Erst wenn Automatismen versagen, zeigt sich das Können der Administratoren. Die Strukturen des Netzes werden zwar immer komplexer, die Grundlagen bleiben aber glücklicherweise gleich. Das vorliegende tecChannel Compact widmet sich diesen Grundlagen und macht Sie fit für die künftigen Netzwerkaufgaben.

In den ersten beiden Kapiteln greifen wir dafür auf Themen aus dem Programm der renommierten Cisco Academy zurück. Genauer gesagt geht es um das Routing in Subnetzen und um virtuelle LANs. Besonders die in sich selbst abgeschlossenen VLANs mausern sich zu einer intelligenten Lösung, wenn verschiedene Netze ohne großen Kostenaufwand voneinander getrennt werden sollen.

Der zweite Themenkomplex geht weg von eigentlichen Verbindungen und beleuchtet Protokolle und Dienste genauer. Neben einem Workshop zur Konfiguration eines Nameservers bringen wir Ihnen das LDAP-Protokoll näher, das im Netzwerk die Brücke zwischen Clients und Verzeichnis-Servern schlägt. Passend dazu ist ein weiterer Beitrag dem Active Directory gewidmet, dem Verzeichnisdienst der Windows-Welt. Wir zeigen Ihnen die häufigsten Katastrophenszenarien samt möglichen Lösungen auf.

Der dritte Bereich des Compacts schließlich dreht sich um die Sicherheit. Samba ist eine der meistgenutzten Lösungen, wenn es um den Datenaustausch in heterogenen Umgebungen geht. Sicher wird das Ganze, wenn Dateizugriffe und Freigaben streng geregelt sind und jeder nur genau das erhält, was er auch haben darf. Unser Beitrag verrät Ihnen, wie Sie diese Zugriffskontrollen effektiv nutzen. Den Abschluss bildet ein Artikel rund um die Sicherheit in Debian/GNU-Linux-Systemen. Mit hilfreicher Zusatzsoftware, gezielten Security-Maßnahmen und vorausschauender Planung läuft auch Ihr System „solid as a rock“.

Viel Spaß beim Lesen wünscht Ihnen

Moritz Jäger
Ressort Software & Netzwerke

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Stellv. Chefredakteur / CvD: Albert Lauchner
Grafik: stroemung, Michael Oliver Rupp, Yvonne Reittinger, Bernd Maier-Leppla
Titelgestaltung: Twentyfirst Communications

Redaktion tecCHANNEL:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897, Fax: -878
Homepage: www.tecChannel.de,
E-Mail: feedback@tecChannel.de
Autoren dieser Ausgabe: William Boswell, Nadine Ebel, Jochen Hein, Frank Ronneburg, John H. Terpstra, Jelmer R. Vernooij
Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Business Verlag GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, vor allem durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags nicht zulässig.
Titelfoto:
Cisco Systems

Anzeigen:
Anzeigenleitung: Dirk Limburg,
Tel.: 0 89/3 60 86-871
Leitung Anzeigendisposition: Rudolf Schuster,
Tel.: 0 89/3 60 86-135, Fax: -99135
Digitale Anzeigenannahme:
Manfred Aumaier, Tel.: 0 89/3 60 86-602,
Andreas Mallin, Tel.: 0 89/3 60 86-603

Vertrieb / Produktion:
Vertrieb: Josef Kreitmair (leitend), Katrin Elsler
Vertriebsmarketing: Peter Priewasser (leitend), Stefanie Kusseler
Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113,
E-Mail: mzv@mzv.de, Website: www.mzv.de
Produktionsleitung: Heinz Zimmermann
Druck: Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in tecCHANNEL-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Business Verlag GmbH ist die IDG Communications Verlag AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA
Verlag: IDG Business Verlag GmbH, Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-0, Fax: -118,
Website: www.idg-verlag.de
Handelsregisternummer: HR 99187
Umsatzidentifikationsnummer: DE 811257800
Geschäftsführer: York von Heimburg
Group Publisher: Stephan Scherzer
Verlagsleitung: Frank Klinkenberg
Vorstand: York von Heimburg, Keith Arnot, Pat Kenealy
Mitglieder der Konzerngeschäftsleitung: Stephan Scherzer, Josef Lohner
Aufsichtsratsvorsitzender:
Patrick J. McGovern

Dieses tecCHANNEL-Compact wurde mit der Adobe Creative Suite CS produziert. tecCHANNEL-Compact erscheint im Verlag der PC-WELT. Zu unserer Verlagsgruppe gehören folgende Zeitschriften:

COMPUTERWOCHE · ComputerPartner · PC WELT · DigitalWorld
Macwelt · GameStar · CIO · gamepro

Leser- und Abo-Service:
Dialog-Service-Center GmbH, Konrad-Zuse-Straße 16, 74172 Neckarsulm, Telefon: 0 18 05/9 99-802, Fax: 0 71 32/9 59-166, E-Mail: tecchannel@d-s-center.de

Inhalt

	Editorial	**3**
	Impressum	**4**
1.	**Grundlagen**	**10**
1.1	**Grundlagen zu Routing und Subnetzbildung**	**10**
1.1.1	Geroutete Protokolle und Routing-Protokolle	11
1.1.2	IP als geroutetes Protokoll	13
1.1.3	Paketübertragung und Switching im Router	14
1.1.4	Verbindungslose Netzwerkdienste	16
	Verbindungsorientierte Netzwerkdienste	17
1.1.5	Aufbau eines IP-Pakets	17
1.1.6	IP-Routing-Protokolle	19
1.1.7	Hauptfunktionen von Routern	19
1.1.8	Routing und Switching im Vergleich	21
	ARP- und Routing-Tabelle	23
1.1.9	Vergleich: Geroutete und Routing-Protokolle	24
1.1.10	Pfadermittlung	26
1.1.11	Adressierung in der Vermittlungsschicht	27
1.1.12	Routing-Tabellen	29
1.1.13	Routing-Algorithmen	30
	Metriken	31
1.1.14	Interne und externe Routing-Protokolle	31
1.1.15	Typen von Routing-Protokollen	32
	Distanzvektor-Protokolle	33
	Link-State-Protokolle	33
1.1.16	Grundlagen der Subnetzbildung	36
1.1.17	IP-Adressklassen	37
1.1.18	Subnetzbildung – Basics	37
1.1.19	Subnetzmaske erstellen	39
1.1.20	Subnetzmaske anwenden	41
1.1.21	Größe der Subnetzmaske bestimmen	42
	Subnetzmaske und IP-Adresse berechnen	43
1.1.22	Subnetze in Klasse-A- und Klasse-B-Netzwerken bilden	44
1.1.23	Netzadresse mit booleschem UND berechnen	45
1.1.24	Fazit	46
1.2	**Einführung in VLANs**	**48**
1.2.1	Logische Gruppen statt physikalischer Segmente	48
1.2.2	Broadcast-Domänen mit VLANs und Routern	50

1.2.3	Betrieb eines VLAN	51
	Portzentrisches statisches VLAN	53
	Ende-zu-Ende-VLANs	54
	Geografische VLANs	55
1.2.4	Vorteile von VLANs	55
1.2.5	VLANs und Sicherheit	56
1.2.6	Hubs und nicht VLAN-fähige Switches	58
1.2.7	VLAN-Typen	59
1.2.8	Kennzeichnung von VLAN-Frames	59
	IEEE 802.1Q (Frame-Tagging)	59
	ISL 60	
	FDDI 802.10	60
	LANE	61
1.2.9	VLAN-Konfiguration	62
	Statische VLANs konfigurieren	62
	Wichtige Regeln	62
1.2.10	Fehlersuche und -behebung bei VLANs	66
	Beispiel zur Fehlersuche	67
	Fehlersuche bei Endstationen	68
1.2.11	Zusammenfassung	69
2.	**Dienste und Services**	**70**
2.1	**Konfiguration und Betrieb eines Nameservers**	**70**
2.1.1	Das Konzept des Domain Name Service	71
2.1.2	Auswahl eines DNS-Servers	72
2.1.3	Allgemeines zur Konfiguration eines Nameservers	72
2.1.4	Primary Nameserver	73
2.1.5	Die Datei named.hosts	74
2.1.6	Das Masterfile-Format	75
	Start Of Authority (SOA)	76
	Nameserver (NS)	77
	Address (A)	77
	Well Known Services (SRV)	78
	Canonical Name (CNAME)	78
	Domain Name Pointer (PTR)	79
	Mail Exchange (MX)	79
	Text (TXT)	80
2.1.7	Die Datei named.local	81
	Die Datei named.rev	81
2.1.8	Slave-Nameserver	83
2.1.9	Weitere Optionen in der Datei named.boot	84
2.1.10	Steuerung des named-Prozesses	85
2.1.11	Betrieb eines Nameservers	86

2.1.12	Dynamische DNS-Updates	87
2.1.13	Sicherheit und DNS	87
	Weitere Informationen zum DNS	89
2.2	**LDAP**	**90**
2.2.1	LDAP-Grundlagen	90
	Abfrageoperationen	91
	Update-Operationen	91
	Authentifizierungs- und Kontrolloperationen	91
2.2.2	LDAP-Modell	94
	Funktionsmodell	95
	Informationsmodell	95
	Namensmodell	95
	Sicherheitsmodell	96
2.2.3	Schema	97
	Objekt-IDs (OIDs)	98
	Attributtypen	99
	Objektklassen	101
2.2.4	LDIF	104
	LDAP-URLs (RFC 1959):	106
2.2.5	LDAP und Sicherheit	107
	Zugriffssteuerung unter LDAP	107
	Authentifizierungsmechanismen	109
	Sicherheitsrisiken bei der Verwendung von LDAP	112
2.2.6	LDAP in der Anwendung	114
	Authentifizierung/Systemverwaltung	114
	Identity Management	115
	Adressbuch	115
2.2.7	LDAP-Tools	115
2.3	**Katastrophenszenarien bei Active Directory**	**117**
2.3.1	Neue Features von Windows Server 2003	117
2.3.2	Ausfall eines DNS-Servers	117
	Folgen eines DNS-Ausfalls für Windows-Clients	118
2.3.4	Ausfall eines Domänencontrollers	119
	Metadaten für einen verlorenen Domänencontroller löschen	121
2.3.5	Ausfall eines FSMO	124
	Übertragung eines FSMO-Rollenmasters	126
	Einen Rollenmaster entziehen	130
2.3.6	Verlust zentraler Replikationskomponenten	131
	Neuen bevorzugten Brückenkopfserver auswählen	132
	ISTG auswählen	133
	Ausfall einer WAN-Leitung	134
2.3.7	Sicherung von Active Directory	134

	Systemstatus-Backup durchführen	136
	Active Directory wiederherstellen	138
2.3.8	Verzeichnis pflegen	145
	Active Directory-Datenbank defragmentieren	146
	Active Directory-Datenbank reparieren	147
3.	**Sicherheit**	**151**
3.1	**Zugriffskontrolle bei Samba und *nix**	**151**
3.1.1	Möglichkeiten und Vorteile	151
	Unix-Datei- und -Verzeichnis-Berechtigungen	152
	Samba-Netzlaufwerksdefinitionen	152
	Samba-Netzlaufwerkskontroll-Listen	152
3.1.2	Die Zugriffskontrollen des Dateisystems	152
	Vergleich zwischen NTFS und dem UNIX-Dateisystem	152
3.1.3	Zugriffskontrollen für Freigabedefinitionen	156
	Benutzer- und gruppen-basierende Kontrollen	156
	Kontrollen, die auf Datei- und Verzeichnis-Berechtigungen basieren	157
	Allgemeine Kontrollen	159
3.1.4	Zugriffskontrollen auf Freigaben	160
	Verwaltung von Freigabeberechtigungen	160
	Windows NT4 Workstation/Server	160
	Windows XP	160
3.1.5	MS Windows-Zugriffskontroll-Listen (ACLs) und UNIX-Wechselwirkungen	161
	Verwalten von UNIX-Berechtigungen durch NT-Sicherheitsdialoge	161
	Anzeigen von Dateisicherheit auf einer Samba-Freigabe	162
	Dateiberechtigungen	163
	Verzeichnis-Berechtigungen	164
	Die Wechselwirkung mit den Samba-Standard-Parametern create mask	165
	Die Wechselwirkung mit den Standard-Samba-Dateiattribut-Vergaben	166
3.1.6	Gängige Fehler	166
3.2	**Systemsicherheit unter Debian GNU/Linux**	**170**
3.2.1	Das Paket task-harden	170
3.2.2	Securing Debian HOWTO	171
	Wichtige Security-Aspekte	172
3.2.3	BIOS-Einstellungen vor der Installation	172
3.2.4	Festplattenpartitionen	172
3.2.5	Administrator Passwort	173
3.2.6	Passwörter und aktivierte Dienste	173

3.2.7	Mailinglisten	174
3.2.8	Absicherung des Bootloaders	174
3.2.9	Starten von Diskette	175
3.2.10	Mounten von Dateisystemen	175
3.2.11	Debian Sicherheitsupdates	176
3.2.12	Pluggable Authentication Modules (PAM)	177
	Password Required	177
	Anmeldung an Terminals	177
	PAM-Kommandos	178
3.2.13	Anpassungen der Datei /etc/inetd.conf	179
3.2.14	Die Datei /etc/login.defs	180
3.2.15	Die Datei /etc/ftpusers	181
3.2.16	Einsatz eines TCP-Wrappers	181
3.2.17	Benutzung von su und sudo	182
3.2.18	Benutzung von chroot	182
3.2.19	Kernel-Features	183
3.2.20	Benutzung der svgalib und sichere Übertragung von Dateien	184
3.2.21	Benutzung von Quota	184
3.2.22	Zugriffsrechte von Logdateien und setuid-Check	185
3.2.23	Kommandos chattr und lsattr	185
3.2.24	Integrität des Dateisystems	186
3.2.25	Die Programme locate und slocate	186
3.2.26	Secure Shell (SSH)	187
3.2.27	FTP-Server	188
3.2.28	X-Anwendungen im Netz	188
3.2.29	Display-Manager	189
3.2.30	E-Mail	189
3.2.31	Loghost – ein Server für Logdateien	190
3.2.32	BIND und Snort	191
3.2.33	Debian-Sicherheits-Updates	192
3.2.34	Austausch von Software	192
3.2.35	Kernel-Patches	192
3.2.36	Cruft	193
3.2.37	Weitere Möglichkeiten	194
3.2.38	Maßnahmen nach einem Einbruch ...	194
3.2.39	Erkennen von Rootkits	195
3.2.40	Rootkit-Tools	195
	Suckit Detection Tool	196
3.2.41	Fazit	196
	Glossar	**109**
	Index	**199**

1. Grundlagen

IP ist das wichtigste im lokalen Netzwerk und im Internet verwendete Protokoll. In diesem Kapitel erläutern wir den Transport von IP-Paketen, die Modifikation des Headers durch Schicht-3-Geräte und den Aufbau eines IP-Pakets. Ferner lernen Sie die Details von verbindungslosen und verbindungsorientierten Netzwerkdiensten kennen. Darüber hinaus erklären wir den Unterschied zwischen Routing-Protokollen sowie gerouteten Protokollen und wie die Netzwerkrouter die Verbindungsstrecken zwischen Standorten optimieren.

Für mehr Sicherheit in Netzwerken soll das Virtual LAN sorgen. Das VLAN unterteilt dabei ein Netzwerk in abgeschirmte Segmente. Dies verbessert auch die Skalierbarkeit und vereinfacht das Netzmanagement. Wir erläutern die Funktionsweise des VLANs im zweiten Beitrag dieses Kapitels.

1.1 Grundlagen zu Routing und Subnetzbildung

Das Internet Protokoll (IP) ist die Grundlage der Protokollfamilie TCP/IP und für die Weiterleitung der Daten zuständig. Generell hat das Internet Protokoll die Aufgabe, die Datenübertragung zwischen Netzwerken sicherzustellen. Der Sender eines IP-Datenpakets kennt dabei zwar die Zieladresse, nicht aber den Weg dorthin.

Jede Station auf dem Weg des Datagramms zum Empfänger muss eine Entscheidung über die Wahl des weiteren Weges fällen. Dieser Vorgang wird als Routing bezeichnet. Sie werden erfahren, worin der Unterschied zwischen Routing-Protokollen und gerouteten Protokollen besteht und wie Router die Entfernung zwischen Standorten ermitteln. Wir werden verschiedene Routing-Ansätze (Distanzvektor-Routing, Link-State-Routing und Hybrid-Routing) vorstellen und zeigen, wie diese Technologien häufige Routing-Probleme lösen.

Durch die Verwendung von Subnetzmasken kann man den Rechneranteil der IP-Adresse in einen Subnetzteil umwandeln. Die Subnetzmaske gibt an, welche Bereiche als Subnetz- und welche als Rechneradresse interpretiert werden. Dadurch schafft man innerhalb eines großen Netzes mehrere kleine, reduziert aber gleichzeitig die Anzahl der Rechner, die zu einem Netz gehören. Diese kleinen Netze innerhalb eines großen Netzes werden als Subnetze bezeichnet.

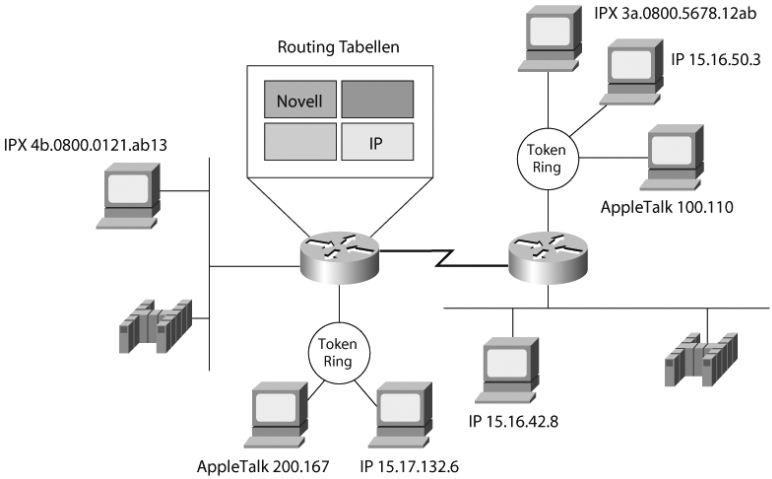
Das IP ist das geroutete Protokoll des Internets. Die IP-Adressierung ermöglicht das Routing von Paketen vom Absender über den optimalen Pfad zum Empfänger. Auch der Transport der Pakete, sich ändernde Kapselungen und verbindungsorientierte wie auch verbindungslose Protokolle sind wesentlich, um sicherzustellen, dass die Daten korrekt zum Ziel übertragen werden. In diesem Artikel wollen wir die genannten Aspekte beschreiben.

1.1.1 Geroutete Protokolle und Routing-Protokolle

Ein Protokoll ist ein auf Standards basierender Satz von Regeln, der bestimmt, wie Computer über Netzwerke miteinander kommunizieren. Ferner dient ein Protokoll auch als gemeinsamer Nenner oder Medium, über das unterschiedliche Anwendungen, Hosts oder Systeme kommunizieren können.

Wenn Computer miteinander kommunizieren, tauschen sie Datenmeldungen aus. Um diese Meldungen in Empfang nehmen und verarbeiten zu können, müssen die Computer wissen, wie die verschiedenen Meldungen definiert sind und was sie bedeuten. Beispiele für Vorgänge, bei denen Meldungen ausgetauscht werden, sind etwa das Herstellen einer Verbindung mit einem entfernten Computer, das Senden und Empfangen von E-Mail und die Übertragung von Daten und Dateien.

Ein Protokoll beschreibt das Format, das eine Meldung aufweisen muss. Zusätzlich bestimmt es die Art und Weise, wie Computer Meldungen innerhalb des Kontexts einer bestimmten Handlung (zum Beispiel beim Übertragen von Nachrichten über ein Netzwerk) austauschen.



Geroutete Protokolle: AppleTalk, IP und Novell IPX (Internetwork Packet Exchange) zählen zu den gerouteten Protokollen.

Aufgrund der Ähnlichkeit von gerouteten beziehungsweise routbaren Protokollen und Routing-Protokollen werden diese Begriffe häufig miteinander verwechselt. Die Begriffe unterscheiden sich folgendermaßen:

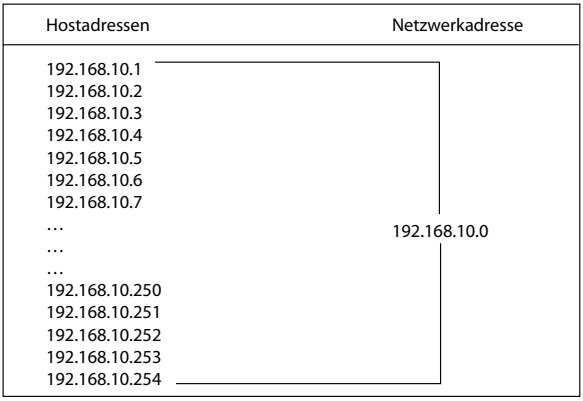
- Als geroutetes Protokoll (auch „routbares“ Protokoll) bezeichnet man jedes Netzwerkprotokoll, in dessen Vermittlungsschichtadresse genug Informationen enthalten sind, um ein Paket auf der Grundlage eines Adresssystems von

einem Host an einen anderen Host weiterzuleiten. Geroutete Protokolle definieren das Format und die Verwendung der Felder in einem System. Die Pakete werden generell von einem Endsystem zum anderen übertragen. Geroutete Protokolle verwenden zur Weiterleitung von Paketen eine Routing-Tabelle.

- Ein Routing-Protokoll hingegen ist ein Protokoll, das den Transport eines gerouteten Protokolls unterstützt, indem es für die Router Methoden zur gemeinsamen Nutzung von Routing-Informationen bereitstellt. Routing-Protokollmeldungen werden zwischen Routern hin- und herbewegt. Routing-Protokolle ermöglichen Routern die Kommunikation mit anderen Routern zum Zweck der Aktualisierung der Tabellen. Beispiele für TCP/IP-Routing-Protokolle sind RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP) und OSPF (Open Shortest Path First).

Zuordnung der Adressen

Damit ein Protokoll routbar ist, muss es in der Lage sein, jedem einzelnen Gerät eine eindeutige Netzwerkadresse sowie eine Host- oder Knotenadresse zuzuweisen. Einige Protokolle wie etwa IPX setzen lediglich voraus, dass ein Administrator eine Netzwerkadresse zuweist; als Hostadresse wird dann die physikalische Adresse (MAC-Adresse) des Hosts verwendet. Andere Protokolle – beispielsweise IP – verlangen jedoch die Angabe einer vollständigen Adresse und einer Subnetzmaske. Sowohl die IP-Adresse als auch die Netzwerkmaske müssen einem gerouteten Netzwerk zugeordnet sein. Eine Netzwerkmaske trennt die 32 Bits umfassende IP-Adresse in einen Netz- und einen Hostanteil auf. IPX benutzt keine Netzwerkmaske, sondern verwendet die mit einer vom Administrator zugewiesenen Netzwerkadresse verknüpfte MAC-Adresse, um die vollständige Adresse zu erstellen. Bei IP-Adressen hingegen wird die Netzwerkadresse durch einen Vergleich der Adresse mit der Netzwerkmaske ermittelt.



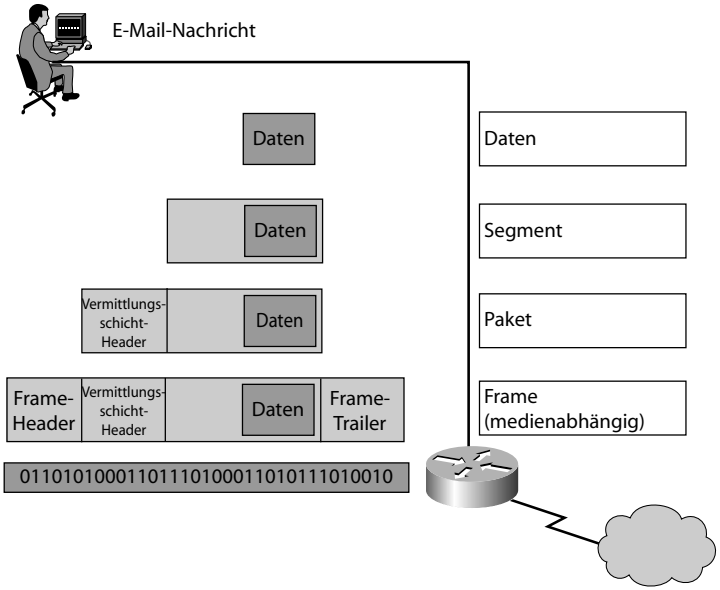
Netzwerk- & Host-Adressen: Alle 254 Hosts lassen sich durch die Netzwerkadresse 192.168.10.0 darstellen.

Eine Netzwerkmaske erlaubt die Behandlung von Gruppen aufeinander folgender IP-Adressen als Einheit. Wenn eine solche Gruppenbildung nicht zulässig wäre, müsste jeder Host zu Routing-Zwecken individuell bekannt sein, was bei den Millionen von Hosts im Internet nicht möglich wäre.

Wie Abbildung zeigt, lassen sich alle 254 Hosts in der Serie 192.168.10.1 bis 192.168.10.254 durch die Netzwerkadresse 192.168.10.0 darstellen. Auf diese Weise können Daten unter Angabe der Netzwerkadresse an jeden beliebigen dieser Hosts gesendet werden; Routing-Tabellen müssen also nur den Eintrag 192.168.10.0 und nicht 254 einzelne Einträge aufweisen. Diese Adressierung entspricht den Vorgaben des ISC (www.isc.org/). Damit das Routing funktioniert, muss diese Form der Gruppenbildung verwendet werden.

1.1.2 IP als geroutetes Protokoll

IP ist die weit verbreiteste Implementierung eines hierarchischen Netzwerkadresssystems. Es handelt sich hierbei um ein verbindungsloses, unzuverlässiges Best-Effort-Transportprotokoll für den Einsatz im Internet. Dabei bedeutet „verbindungslos“, dass keine dedizierte Verbindung vorhanden sein muss – anders als etwa bei einem Telefonanruf.



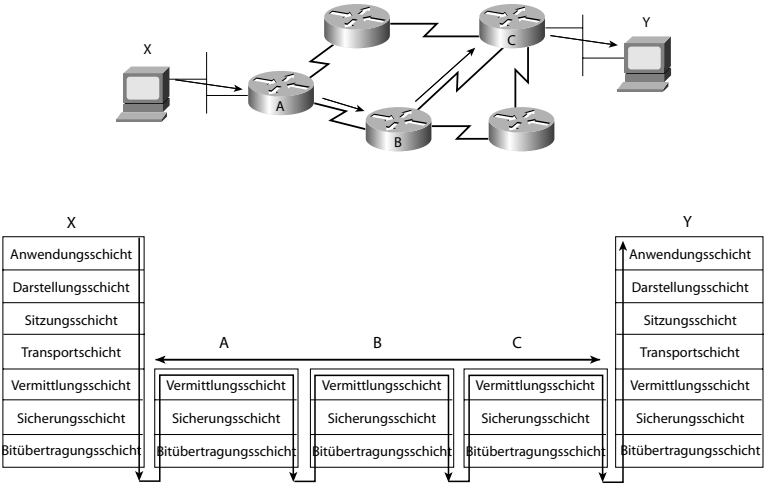
Kapselung: Wenn die Daten den OSI-Protokollstapel durchlaufen, werden sie in jeder Schicht bearbeitet. In der Vermittlungsschicht werden sie in Paketen gekapselt, die auch Datagramme heißen.

Vor der Übertragung der Daten zwischen den Hosts findet also keine Rufkonfiguration statt: Das IP-Protokoll verwendet die entsprechend den Entscheidungen des Routing-Protokolls beste Route. Die Attribute „unzuverlässig“ und „Best Effort“ sollen nicht andeuten, dass das Protokoll unsicher und wenig effizient ist, sondern signalisieren lediglich, dass IP keinen Versuch unternimmt, um festzustellen, ob ein Paket ordnungsgemäß ausgeliefert wurde; solche Funktionen werden vielmehr von Protokollen der oberen Schichten realisiert.

IP bestimmt die Form des IP-Paket-Headers (der Adress- und Steuerinformationen enthält), befasst sich jedoch nicht mit den eigentlichen Daten, sondern akzeptiert alles, was ihm von den übergeordneten Schichten übermittelt wird.

1.1.3 Paketübertragung und Switching im Router

Wenn ein Paket durch ein Netzwerk zu seinem Empfänger übertragen wird, werden Header und Trailer des Frames durch jeden Router (Schicht-3-Gerät) ersetzt. Der Grund hierfür ist die Tatsache, dass Schicht-2-Einheiten (Frames) der lokalen Adressierung dienen, Schicht-3-Einheiten (Pakete) hingegen für die Ende-zu-Ende-Adressierung zum Einsatz kommen.



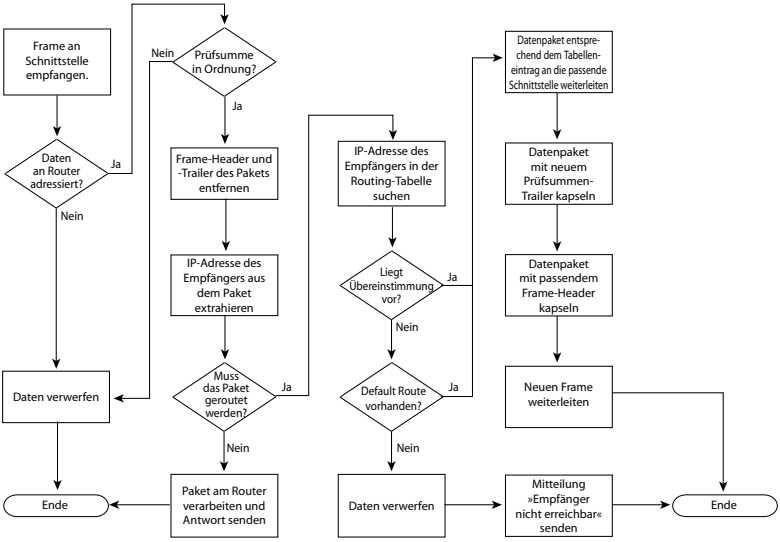
Im Fluss: Die Abbildung zeigt den Datenfluss in einem Gerät der Vermittlungsschicht.

Ethernet-Frames der Schicht 2 sollen innerhalb einer Broadcast-Domäne funktionieren und mit den MAC-Adressen arbeiten, die den physischen Geräten zugewiesen sind. Zu anderen Typen der Schicht-2-Frames gehören serielle Punkt-zu-Punkt-Verbindungen und Frame-Relay-Verbindungen in WANs, die ein eigenes Schicht-2-Adressierungssystem verwenden. Der wesentliche Aspekt ist hier, dass

unabhängig davon, welches Adressierungssystem verwendet wird, dieses nur innerhalb der Schicht-2-Broadcast-Domäne zum Einsatz kommt. Sobald die Daten ein Schicht-3-Gerät passieren, werden die Schicht-2-Informationen geändert.

Routing-Prozedur

Wenn ein Frame an der Router-Schnittstelle ankommt, wird die MAC-Adresse extrahiert und überprüft, um festzustellen, ob der Frame direkt an die Schnittstelle gerichtet oder ein Broadcast ist (diese Vorgehensweise ist bei allen Geräten in einer Kollisionsdomäne die gleiche). In diesen beiden Fällen wird das Paket akzeptiert, in jedem anderen verworfen, weil es für ein anderes Gerät in der Kollisionsdomäne bestimmt war. Nun wird die CRC-Prüfsumme aus dem Frame-Trailer extrahiert und berechnet, um sicherzustellen, dass der Frame fehlerfrei an der Schnittstelle ankam. Schlägt die Überprüfung fehl, so wird der Frame ebenfalls verworfen. Andernfalls erfolgt die Entfernung von Header und Trailer und der Frame wird an Schicht 3 übergeben.



Routing-Prozedur: Links oben im Bild kommt ein Frame an der Router-Schnittstelle an und wird verarbeitet.

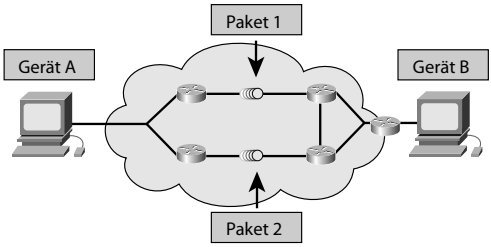
In der Vermittlungsschicht wird das Paket dann überprüft, um festzustellen, ob es direkt an den Router gerichtet ist oder an ein anderes Gerät im Netzwerk weitergeleitet werden muss. Die Pakete, die direkt für den Router bestimmt sind, enthalten als Empfängeradresse die IP-Adresse eines Router-Ports. Ist dies der Fall, dann wird der Schicht-3-Header entfernt und das Paket an Schicht 4 übergeben. Soll das Paket jedoch geroutet werden, dann wird die Empfänger-IP-Adresse in der

Routing-Tabelle ermittelt. Wird eine Übereinstimmung gefunden oder gibt es eine Default-Route, dann wird das Paket über die Router-Schnittstelle gesendet, die in der Tabelle angegeben ist. Wenn das Paket zum Ausgangsport geswitcht wurde, wird ein neuer CRC-Wert als Frame-Trailer hinzugefügt und je nach Schnittstellentyp (Ethernet, seriell oder Frame Relay) ein passender Frame-Header an den Anfang des Pakets gesetzt. Dann wird der Frame in die nächste Broadcast-Domäne gesendet, um seinen Weg zum endgültigen Empfänger fortzusetzen.

1.1.4 Verbindungslose Netzwerkdienste

Die meisten Netzwerkdienste verwenden ein verbindungsloses Transportsystem, das heißt, sie behandeln jedes eingehende Paket für sich und schicken es auf seinen Weg durch das Netzwerk. Dabei kann es zwar sein, dass die Pakete unterschiedliche Wege durch das Netzwerk nehmen, aber beim Empfänger werden sie wieder in der korrekten Reihenfolge zusammengesetzt. In einem verbindungslosen System wird der Empfänger vor dem Versand des Pakets nicht kontaktiert.

Eine Analogie für ein verbindungsloses System ist das Postsystem. Der Empfänger wird (normalerweise) vom Absender nicht kontaktiert, bevor dieser einen Brief an ihn verschickt. Welchen Weg der Brief nimmt, ist weder für den Absender noch für den Empfänger von Belang, und der Empfänger erfährt von dem Brief meist erst, wenn dieser eintrifft.



Verbindungsloser Transport: Jedes eingehende Paket wird für sich behandelt und auf den Weg geschickt.

Verbindungslose Netzwerkprozesse werden oft auch als paketvermittelte Prozesse bezeichnet. Bei diesen Prozessen können Pakete, wenn sie vom Absender an den Empfänger geschickt werden, nicht nur unterschiedliche Wege nehmen, sondern sie kommen (möglicherweise) auch in der falschen Reihenfolge an. Netzwerkgeräte ermitteln den besten Pfad basierend auf Kriterien, die sich während des Versands von Paket zu Paket ändern können (beispielsweise kann die verfügbare Bandbreite die Pfadermittlung beeinflussen).

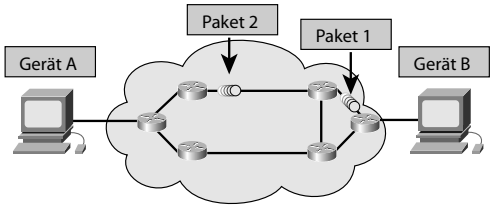
Das Internet ist ein riesiges verbindungsloses Netzwerk, in dem der gesamte Pakettransport über IP abgewickelt wird. TCP (Schicht 4) ergänzt den IP-Transport mit verbindungsorientierten und zuverlässigen Diensten. TCP-Segmente werden für den Transport über das Internet in IP-Pakete gekapselt.

IP ist ein verbindungsloses Protokoll, das heißt, es behandelt jedes Paket individuell. Wenn Sie also beispielsweise mit einem FTP-Programm eine Datei herunterladen, dann schickt IP diese Datei nicht in einem langen, ununterbrochenen Datenstrom, sondern paketweise. Jedes Paket kann dabei andere Wege nehmen, und das eine oder andere kann sogar verloren gehen. IP überlässt es dem Transportschichtprotokoll festzustellen, ob Pakete verloren gegangen sind und neu übermittelt werden müssen. Ferner ist die Transportschicht auch für die Wiederzusammensetzung der Pakete zuständig.

Verbindungsorientierte Netzwerkdienste

Im Gegensatz zu den verbindungslosen Diensten wird in den verbindungsorientierten Systemen vor dem Versand von Daten eine Verbindung zwischen dem Absender und dem Empfänger hergestellt.

Verbindungsorientierter Transport: Vor dem Versand von Daten wird eine Verbindung zwischen Absender und Empfänger hergestellt.

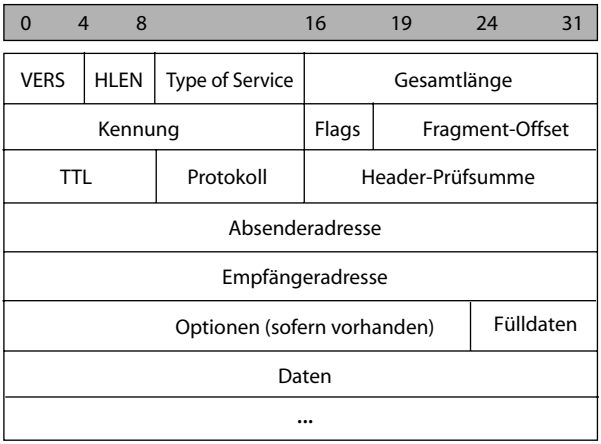


Ein Beispiel für ein verbindungsorientiertes Netzwerk ist das Telefonnetz. Wenn Sie jemanden anrufen, wird eine Verbindung zwischen zwei Telefonanschlüssen hergestellt – erst dann kann die Kommunikation beginnen. Bei verbindungsorientierten Netzwerkprozessen beginnt der Datentransfer nach Herstellung der Verbindung. Alle Pakete wandern nacheinander über dieselbe physikalische Leitung oder – häufiger – dieselbe virtuelle Verbindung.

1.1.5 Aufbau eines IP-Pakets

Wir wissen bereits, dass Pakete (oder Datagramme) der Schicht 3 in der Schicht 2 (Sicherungsschicht) zu Frames gekapselt werden. Ähnlich setzt sich auch das IP-Paket zusammen, das aus den Daten der übergeordneten Schichten sowie einem Header besteht. Der IP-Header besteht aus den folgenden Feldern:

- Version. Zeigt die verwendete IP-Version an. Alle Geräte müssen mit derselben IP-Version arbeiten; Geräte mit anderen Versionen würden die Pakete dagegen verwerfen (4 Bit).
- IP-Header-Länge (HLEN). Es handelt sich um die Gesamtlänge der Header-Daten, die aufgrund zweier unterschiedlich langer Header-Felder angegeben werden muss (4 Bit).



Inhalt eines IP-Pakets: Die Header-Daten beschreiben die Eigenschaften eines IP-Pakets, es folgen die eigentlichen Daten.

- Type of Service. Dieses Feld gibt den Prioritätsgrad des Pakets an, der von einem speziellen übergeordneten Protokoll zugewiesen wird (8 Bit).
- Gesamtlänge. Gibt die Länge des gesamten IP-Pakets einschließlich der Daten und des Headers in Byte an. Um den Umfang der Nutzdaten zu bestimmen, ziehen Sie den HLEN-Wert von der Gesamtlänge ab (16 Bit).
- Kennung. Eine enthaltene Zahl kennzeichnet das Datagramm (16 Bit).
- Flags. Hierbei handelt es sich um ein drei Bit langes Feld, in dem die beiden niederwertigen Bits die Fragmentierung steuern. Ein Bit legt fest, ob das Paket fragmentiert werden darf, das zweite gibt an, ob dieses Paket das letzte Fragment einer Serie von fragmentierten Paketen ist (3 Bit).
- Fragment-Offset. Ermöglicht die korrekte Zusammensetzung von Datagrammfragmenten. Zweck des Feldes ist es, das Flags-Feld an einer 16-Bit-Grenze enden zu lassen (13 Bit).
- TTL (Time-to-Live). Enthält einen Zählerwert, der sich bei jedem Hop (Router) um den Wert „1“ verringert. Wenn der Zähler den Wert „0“ erreicht, wird das Datagramm ungültig und deswegen verworfen. Dadurch wird verhindert, dass Datagramme endlos im Netzwerk kreisen (8 Bit).
- Protokoll. Zeigt an, welches Protokoll auf der übergeordneten Schicht (zum Beispiel TCP oder UDP) die eingehenden Pakete nach Abschluss der IP-Verarbeitung erhält (8 Bit).
- Header-Prüfsumme. Sicherstellung der Integrität des IP-Headers (16 Bit)
- Absenderadresse. Gibt die IP-Adresse des Absenders an (32 Bit).
- Empfängeradresse. Gibt die IP-Adresse des Empfängers an (32 Bit).

- Optionen. Ermöglicht die Unterstützung verschiedener Option, z. B. Sicherheitsfunktionen (Länge variabel).
- Fülldaten. Fügt zusätzliche Nullen hinzu, um sicherzustellen, dass der IP-Header immer ein Vielfaches von 32 Bit ist.
- Daten. Daten der übergeordneten Schicht (Länge variabel, max. 64 KByte).

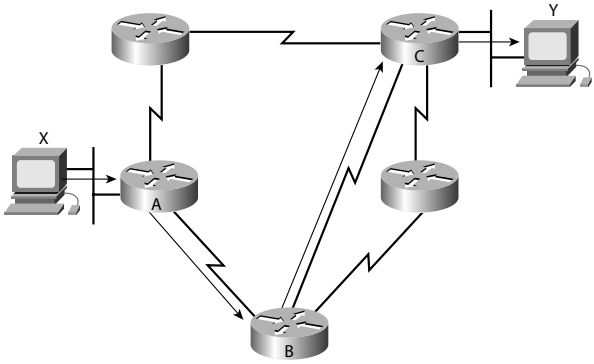
1.1.6 IP-Routing-Protokolle

Routing-Protokolle ermöglichen Routern die Kommunikation mit anderen Routern zum Zweck der Aktualisierung von Tabellen, auf deren Basis sie den besten Pfad zu einem Host im Netzwerk finden können. Routing fungiert als hierarchisches Organisationssystem. Es ermöglicht die Zusammenfassung einzelner Adressen zu Gruppen und deren Behandlung als Einheit, bis die tatsächliche Endadresse für die Auslieferung der Daten an den eigentlichen Empfänger benötigt wird. Unter dem Begriff „Routing“ versteht man die Ermittlung des effizientesten Pfades von einem Gerät zum anderen. Das Hauptgerät, das diesen Vorgang durchführt, bezeichnet man als Router.

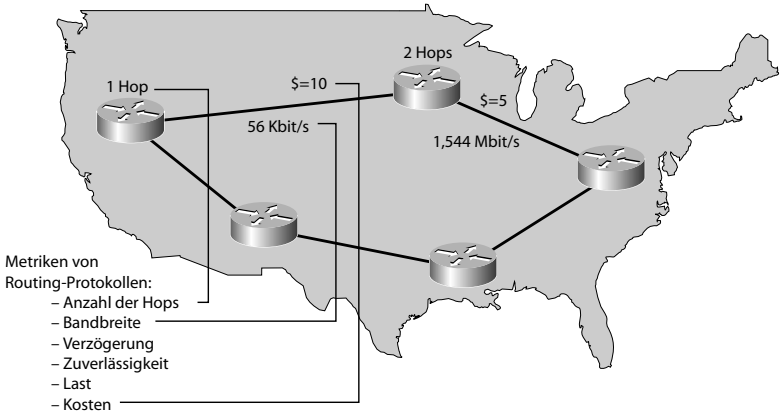
1.1.7 Hauptfunktionen von Routern

Router haben im Prinzip zwei Hauptfunktionen. Sie müssen zum einen Routing-Tabellen führen und sicherstellen, dass andere Router von Änderungen in der Netzwerktopologie erfahren. Diese Funktion wird mit einem Routing-Protokoll realisiert, das Änderungen anderen Routern mitteilt. Wenn Pakete an der Schnittstelle eintreffen, bestimmt der Router zum anderen anhand der Routing-Tabelle, wohin diese weitergeleitet werden müssen. Er überträgt sie an die passende Schnittstelle, ergänzt das hierfür notwendige Framing und sendet den Frame.

Wegsuche: Unter dem Begriff „Routing“ versteht man die Ermittlung des effizientesten Pfades von einem Gerät zum anderen.



Ein Router ist ein Gerät der Vermittlungsschicht, das eine oder mehrere Routing-Metriken zur Bestimmung des optimalen Pfades verwendet, über den die Netzwerkdaten weitergeleitet werden sollen. Unter der Metrik versteht man einen Wert, der angibt, wie wünschenswert die Übertragung über eine bestimmte Schnittstelle ist. Routing-Protokolle verwenden verschiedene Kombinationen von Kriterien, um die Metrik zu ermitteln.



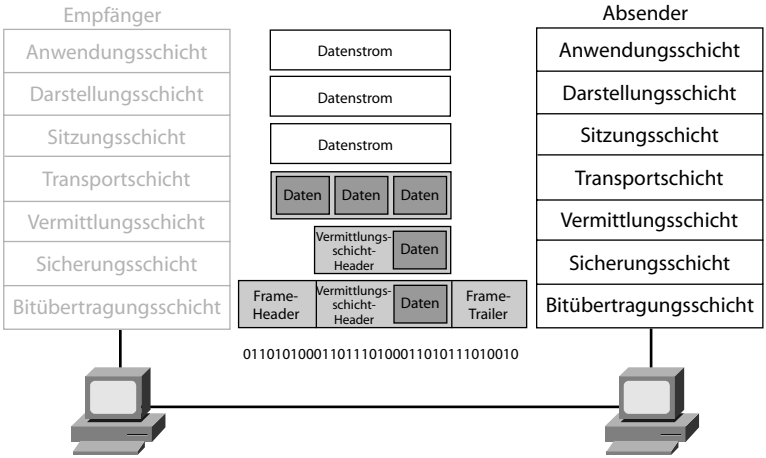
Metriken von Routing-Protokollen: Der Metrik-Wert gibt Priorität der Übertragung über eine bestimmte Schnittstelle an.

Metriken wie die Anzahl der Hops, Bandbreite, Verzögerung, Zuverlässigkeit, Last und Kosten werden in unterschiedlichen Kombinationen berechnet, um den besten Pfad durch einen Netzwerkverbund zu bestimmen. Router verbinden Netzwerksegmente oder ganze Netzwerke miteinander. Sie leiten Daten-Frames basierend auf den Informationen der Schicht 3 zwischen Netzwerken weiter.

Kapselung von Paketen

Router treffen hinsichtlich des besten Transportpfades für Daten in einem Netzwerkverbund logische Entscheidungen. Dabei führt der Router die Weiterleitung der Pakete zu den geeigneten Ausgangsports durch, wo sie dann für die Übertragung gekapselt werden.

Bei der Kapselung wird der Datenstrom in Segmente unterteilt, die passenden Header und Trailer werden hinzugefügt, und dann werden die Daten gesendet. Bei der Entkapselung geschieht das Umgekehrte, d.h., die Header und Trailer werden entfernt, und dann werden die Daten wieder zu einem kontinuierlichen Datenstrom zusammengefügt. Router akzeptieren Frames von LAN-Geräten (zum Beispiel Workstations) und leiten diese basierend auf der Schicht-3-Information dann weiter durch das Netzwerk.



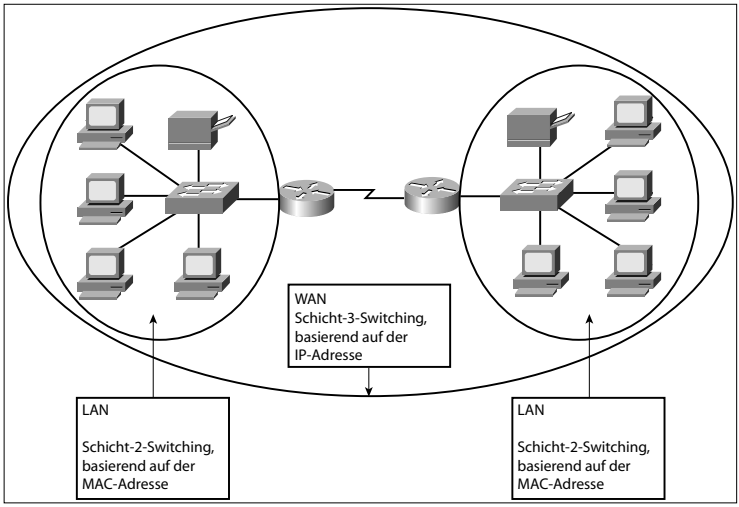
Ein- und Auspacken: Der Kapselungs-/Entkapselungsprozess findet jedes Mal statt, wenn ein Paket einen Router passiert und die Daten von einem Gerät zum nächsten übertragen werden.

Es ist wichtig zu wissen, dass es auch andere geroutete Protokolle gibt, so etwa IPX/SPX und AppleTalk. IP und die anderen gerouteten Protokolle bieten Unterstützung für die Schicht 3 und sind insofern routbare Protokolle. Es gibt auch andere Protokolle, welche die Vermittlungsschicht nicht unterstützen; diese heißen „nicht geroutete" Protokolle. Das gängigste Beispiel für solche Protokolle ist NetBEUI (NetBIOS Extended User Interface. Hierbei handelt es sich um ein kleines, schnelles und effizient arbeitendes Protokoll, dessen Einsatz aus genau diesen Gründen auf ein Segment beschränkt ist.

1.1.8 Routing und Switching im Vergleich

Routing wird oft dem Switching in Schicht 2 gegenübergestellt und mag dem flüchtigen Beobachter als mehr oder weniger identische Funktionalität erscheinen. Der wesentliche Unterschied zwischen den beiden Funktionen besteht darin, dass das Switching in Schicht 2 (Sicherungsschicht) des OSI-Modells stattfindet, das Routing hingegen in Schicht 3. Dieser Unterschied bedeutet, dass Routing und Switching bei der Weiterleitung von Daten von einem Absender an einen Empfänger unterschiedliche Informationen verwenden.

Die Beziehung zwischen Switching und Routing ähnelt dem zwischen einem Orts- und einem Ferngespräch beim Telefonieren. Wenn ein Anruf bei einem anderen örtlichen Teilnehmer (das heißt einem Teilnehmer mit identischer Ortsvorwahl) gemacht wird, dann wird dieser über einen lokalen Switch vermittelt. Dieser Switch kann sich jedoch nicht alle Telefonnummer in der ganzen Welt merken, sondern nur die lokalen Nummern speichern.



In Schichten: Switching erfolgt in Schicht 2 und Routing in der Schicht 3.

Empfängt er dann einen Anruf für einen Teilnehmer außerhalb des lokalen Bereichs, dann leitet er diesen an einen anderen Switch weiter, der auf einer höheren Ebene agiert und Ortsvorwahlen kennt. Dieser übergeordnete Switch schaltet den Anruf dann so, dass er letzten Endes über den lokalen Switch geführt wird, dessen Ortsbereich die gewählte Ortskennzahl zugeordnet ist.

Router arbeitet in höherer Schicht

Der Router hat eine Funktion, die der des übergeordneten Switchs im Telefonnetz ähnelt. Das Schicht-2-Switching findet innerhalb des LAN (Broadcast-Domäne) statt, während das Routing in Schicht 3 Daten zwischen Broadcast-Domänen weiterleitet. Dies macht ein hierarchisches Adressierungssystem notwendig, und ein solches System wird in Schicht 3 über das IP-Protokoll bereitgestellt.

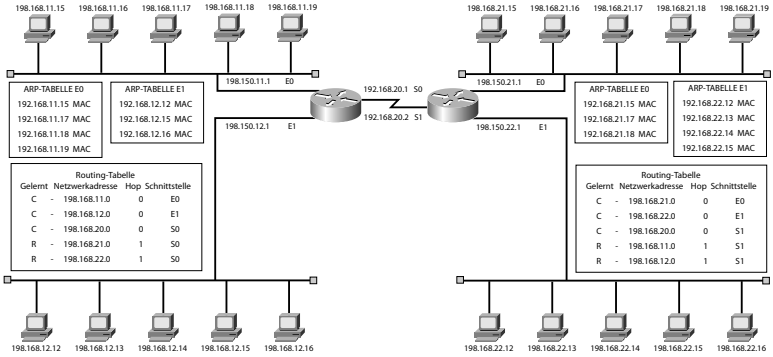
Der Schicht-2-Switch kann nur lokale MAC-Adressen, nicht jedoch die IP-Adressen der Schicht 3 verarbeiten. Wenn ein Host Daten an eine nicht lokale IP-Adresse übertragen will, dann sendet er den Frame an sein Default-Gateway, den Router, indem er dazu die MAC-Adresse des Routers als Empfänger verwendet.

Ein Schicht-2-Switch verbindet Segmente miteinander, die dem gleichen logischen Netzwerk oder Subnetz angehören. Wenn ein Host X einen Frame an einen Host in einem anderen Netzwerk oder Subnetz übertragen will, dann schickt er den Frame an den Router, der auch mit dem Switch verbunden ist. Host X kennt die IP-Adresse des Routers, weil die IP-Konfiguration des Hosts auch die IP-Adresse des Default-Gateways enthält; die MAC-Adresse des Routers hingegen kennt er (noch) nicht. Diese erfährt er mithilfe einer ARP-Anfrage, die für eine IP-Adresse die MAC-Adresse liefert.

Der Switch leitet den Frame aufgrund der gespeicherten Empfänger-MAC-Adresse an den Router weiter. Der Router untersucht nun die Empfängeradresse des Pakets in Schicht 3, um eine Entscheidung zur Weiterleitung zu treffen. Das Default-Gateway ist die Schnittstelle des Routers, die an das gleiche Netzwerk oder Subnetz angeschlossen ist wie Host X.

ARP- und Routing-Tabelle

Ähnlich, wie ein Switch eine Tabelle bekannter MAC-Adressen führt, arbeitet auch ein Router mit einer Tabelle, welche die IP-Adressen der ihm bekannten Netzwerke enthält. Eine solche Tabelle heißt Routing-Tabelle. Jede Ethernet-Schnittstelle an einem Computer oder Router führt eine ARP-Tabelle für die Kommunikation in Schicht 2. Die ARP-Tabelle ist allerdings nur für die Broadcast-Domäne gültig, an die das betreffende Gerät angeschlossen ist. Der Router hat zudem eine Routing-Tabelle, mit deren Hilfe er Daten aus der Broadcast-Domäne heraus routen kann. Jede ARP-Tabelle enthält das betreffende Paar aus IP- und MAC-Adresse. Die Routing-Tabellen enthalten Angaben dazu, wie die Route im jeweiligen Fall erlernt wurde (C steht für eine direkte Verbindung, R für ein Erlernen durch das RIP-Protokoll), welche Netzwerkadresse das jeweilige Netzwerk hat, wie viele Hops bis zu diesem Netzwerk zurückzulegen sind und über welchen Port die Daten gesendet werden müssen, um zum Empfängernetzwerk zu gelangen.



ARP-Tabellen im Router: Jede Ethernet-Schnittstelle an einem Computer oder Router führt eine ARP-Tabelle für die Kommunikation in Schicht 2.

Der Unterschied zwischen den beiden Adresstypen besteht darin, dass MAC-Adressen auf keine besondere Weise organisiert sind. Das ist auch sinnvoll, weil jedes einzelne Netzwerksegment keine große Zahl von Hosts hat, also durchaus leicht zu verwalten ist. Würden allerdings IP-Netzwerkadressen auf die gleiche Weise behandelt, dann würde das Internet nicht funktionieren. Es gäbe keine Möglichkeit, all die Adressen und Pfade zu diesen Adressen zu organisieren – sei es hierarchisch oder auf eine andere Weise.

Die Organisation der IP-Adressen erlaubt jedoch die Gruppierung der Adressen, um diese als Einheit zu behandeln; erst wenn ein bestimmter Host in einem Netzwerk identifiziert werden muss, muss diese Gruppierung aufgelöst werden. Stellen Sie sich diesen Sachverhalt wie eine Bücherei vor, in der Millionen einzelner Buchseiten auf einem großen Haufen aufgeschichtet sind. All dieses Material ist nutzlos, weil es unmöglich ist, ein einzelnes Dokument ausfindig zu machen. Wenn die Seiten zu Büchern zusammengefasst würden und jede Seite eindeutig markiert wäre und wenn die Bücher dann noch in einem Bibliothekskatalog aufgelistet wären, dann wäre es viel einfacher, Daten zu finden und zu verwenden.

Router bieten mehr Sicherheit

Ein weiterer Unterschied zwischen geswitchten und gerouteten Netzwerken besteht darin, dass geswitchte Schicht-2-Netzwerke Schicht-3-Broadcasts nicht blockieren. Daraus ergibt sich jedoch, dass solche Netzwerke Broadcast-Stürmen zum Opfer fallen können. Router hingegen blockieren Broadcasts normalerweise, sodass ein Broadcast-Sturm nur die Domäne beeinträchtigen kann, aus der er stammt. Router bieten zudem, weil sie Broadcasts blockieren, mehr Sicherheit und bessere Bandbreitenkontrolle als Schicht-2-Switches.

Router und Switches im Vergleich		
Funktion	**Router**	**Switch**
Geschwindigkeit	langsamer	schneller
OSI-Schicht	Schicht 3	Schicht 2
Adressierungssystem	IP	MAC
Broadcasts	werden blockiert	werden weitergeleitet
Sicherheit	höher	niedriger
Netzwerksegmentierung	segmentiert Broadcast-Domänen	segmentiert Kollisionsdomänen

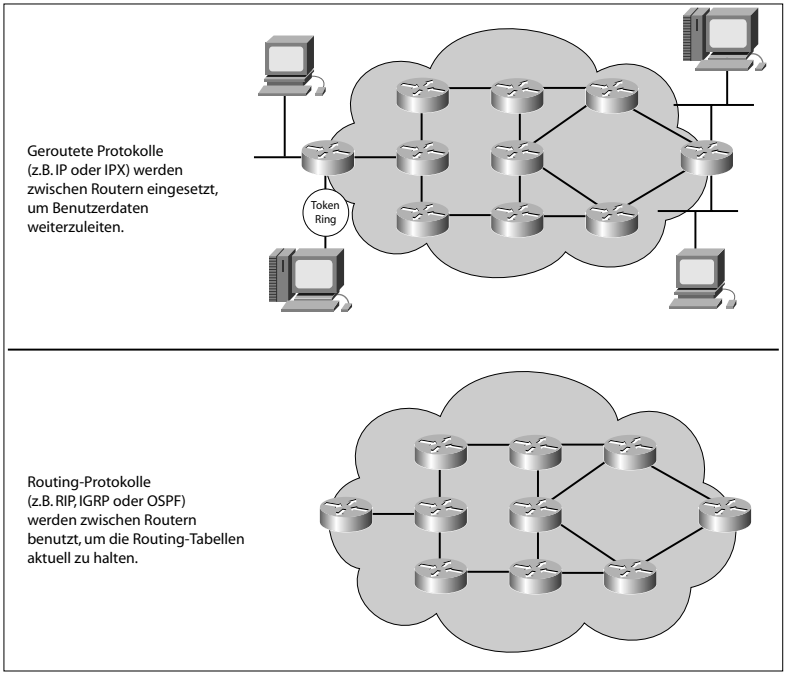
1.1.9 Vergleich: Geroutete und Routing-Protokolle

In der Vermittlungsschicht werden hier zwei Protokollkategorien verglichen, nämlich geroutete Protokolle und Routing-Protokolle. Geroutete Protokolle transportieren Daten durch ein Netzwerk, während es Routing-Protokolle Routern ermöglichen, Daten optimal von einem Standort zu einem anderen weiterzuleiten. Protokolle, die Daten von einem Host über einen Router zu einem anderen Host übertragen, sind geroutete Protokolle (oder auch „routbare“ Protokolle):

- Es geht um eine beliebige Netzwerkprotokollfamilie, die genug Informationen in der Vermittlungsschicht enthält, um es Routern zu ermöglichen, das Paket an das nächste Gerät auf dem Weg zu seinem Empfänger weiterzuleiten.

- Es definiert Format und Verwendung der Felder in einem Paket. Pakete werden normalerweise von Endsystem zu Endsystem befördert.

IP und IPX sind geroutete Protokolle. Weitere Beispiele sind DECnet, Apple¬Talk, Banyan VINES und XNS (Xerox Network Systems).



Unterschiede: Geroutete Protokolle und Routing-Protokolle haben verschiedene Aufgaben.

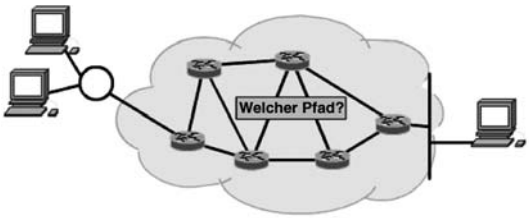
Im Gegensatz zu gerouteten Protokollen verwenden Router Routing-Protokolle, um Routing-Tabellen auszutauschen und Routing-Informationen gemeinsam zu verwenden. Mit anderen Worten: Routing-Protokolle erlauben Routern das Routing gerouteter Protokolle, nachdem ein optimaler Pfad ermittelt wurde. Ein Routing-Protokoll hat folgende Funktion:

- Es stellt Prozesse zur gemeinsamen Nutzung von Informationen bereit.
- Es ermöglicht Routern die Kommunikation mit anderen Routern zwecks Aktualisierung und Wartung der Routing-Tabellen.

Zu den Routing-Protokollen, die mit IP geroutete Protokolle unterstützen, gehören RIP, IGRP, OSPF, BGP (Border Gateway Protocol) und EIGRP.

1.1.10 Pfadermittlung

Die Pfadermittlung erfolgt in der Schicht3 (Vermittlungsschicht). Sie erlaubt einem Router, die möglichen Pfade zu einem Ziel zu bewerten und die bevorzugte Verarbeitungsmethode für ein Paket festzulegen. Routing-Dienste verwenden Netzwerktopologiedaten zur Bestimmung der Netzwerkpfade. Die Pfadsuche ist der Vorgang, bei dem ein Router den nächsten Hop auf dem Weg zum Bestimmungsort eines Pakets ermittelt. Man sagt auch, dass ein Paket geroutet wird.



Pfadwahl: Routing-Dienste verwenden Netzwerktopologiedaten zur Bestimmung der Netzwerkpfade.

Die Pfadsuche für ein Paket kann mit einem Autofahrer verglichen werden, der von einer Seite der Stadt zur anderen fährt. Der Fahrer hat eine Karte, die ihm zeigt, über welche Straßen er zum Ziel gelangt. Die Fahrt von einer Kreuzung zu einer anderen kann man als Hop betrachten.

Auch ein Router verwendet eine Karte, welche die vorhandenen Wege zu einem Zielort darstellt. Router können ihre Entscheidungen zudem auf der Basis der Datendichte und der Geschwindigkeit einer Verbindung (Bandbreite) treffen, so wie der Fahrer vielleicht eine gut ausgebaute Straße den schmalen Gassen durch Wohngebiete vorziehen würde, auch wenn die Verwendung letzterer von der Entfernung her vielleicht geeigneter wäre.

Ähnlich treffen Router ihre Entscheidungen basierend auf der Last, der Bandbreite, der Latenz, den Kosten und der Zuverlässigkeit einer Netzwerkleitung. Der folgende Vorgang beschreibt, wie der Pfad für jedes einzelne Paket ermittelt wird:

- Aus dem Paket wird die Empfängeradresse ausgelesen.
- Die Maske des ersten Eintrags in der Routing-Tabelle wird auf die Empfängeradresse angewendet. Dann werden die maskierte Empfängeradresse und der Eintrag der Routing-Tabelle miteinander verglichen: Liegt eine Übereinstimmung vor, dann wird das Paket an den Port weitergeleitet, der mit diesem Tabelleneintrag verknüpft ist. Liegt keine Übereinstimmung vor, dann wird der nächste Tabelleneintrag geprüft.
- Kann das Paket keinem Eintrag in der Tabelle zugeordnet werden, dann prüft der Router, ob eine Default-Route vorhanden ist (eine Default-Route ist eine Route, die vom Netzwerkadministrator konfiguriert wird und über die alle Pakete gesendet werden, für die kein Eintrag in der Routing-Tabelle gefunden

werden kann): Ist dies der Fall, dann wird das Paket an den entsprechenden Port weitergeleitet. Ist keine Default-Route vorhanden, dann wird das Paket verworfen. Häufig wird in diesem Fall an das sendende Gerät eine Meldung geschickt, dass der Empfänger nicht erreichbar ist.

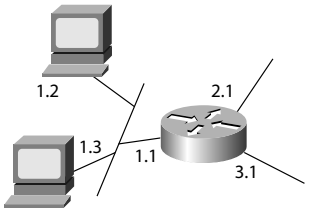
1.1.11 Adressierung in der Vermittlungsschicht

Die Netzadresse hilft dem Router bei der Bestimmung eines Pfades in der Netzwerkwolke und bietet zudem hierarchische oder Subnetzinformationen. Der Router ermittelt anhand dieser Adresse das Empfängernetzwerk eines Pakets innerhalb eines Netzwerkverbundes. Zusätzlich zur Netzadresse verwenden Netzwerkprotokolle aber auch eine Hostadresse (oder Netzknotenadresse).

Für einige Protokolle der Vermittlungsschicht muss der Netzwerkadministrator Hostadressen entsprechend der Vorgabe eines Netzadressierungsschemas zuweisen. Bei anderen Protokollen wiederum erfolgt diese Hostadresszuweisung teilweise oder vollständig automatisch oder dynamisch.

Netzadressen: Die Abbildung zeigt drei Geräte in Netzwerk 1 (zwei Workstations und einen Router), die jeweils eine eigene eindeutige Hostadresse haben. Ferner zeigt die Abbildung, dass der Router mit zwei weiteren Netzwerken (Netzwerk 2 und Netzwerk 3) verbunden ist.

Netzwerk	Host
1	1 2 3
2	1
3	1



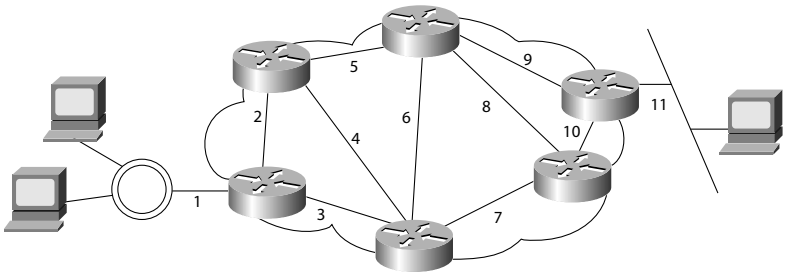
Die logische Adressierung findet in der Vermittlungsschicht statt. Wenn wir uns die Analogie zum Telefonnetz noch einmal ins Gedächtnis rufen, dann entspricht der Netzanteil der IP-Adresse der Vorwahl, während die Anschlussnummer den Geräten des Netzbetreibers mitteilt, an welchen Anschluss innerhalb eines Ortsbereichs der Anruf weiterzuleiten ist. Insofern ähnelt die Anschlussnummer dem Hostanteil einer IP-Adresse, denn dieser Hostanteil teilt dem Router mit, an welches Gerät das Paket auszuliefern ist.

Ohne Adressierung in der Vermittlungsschicht kann das Routing nicht durchgeführt werden. Router benötigen die Netzadressen, um die Pakete korrekt ausliefern zu können. Erst eine hierarchische Adressierungsstruktur ermöglicht die Übertragung von Paketen zwischen den Netzwerken. Schließlich wäre ohne hierarchische Strukturen bei Telefonnummern, Postadressen und Transportsystemen eine moderne Kommunikation und Logistik auch nicht denkbar.

Eine MAC-Adresse kann in diesem Zusammenhang mit dem Namen einer Person verglichen werden, während die Adresse in der Vermittlungsschicht (Netzwerk- und Hostadresse) der Postadresse entspräche. Wenn Sie beispielsweise in eine andere Stadt ziehen, dann würde Ihr Name sich nicht ändern – anders als die Postadresse, die Ihren neuen Standort repräsentieren würde. Netzwerkgeräte (Router wie auch einzelne Computer) haben sowohl eine MAC-Adresse als auch eine Protokolladresse (Adresse in der Vermittlungsschicht). Wenn Sie einen Computer in einem anderen Netzwerk anschließen, dann bleibt seine MAC-Adresse gleich, aber er benötigt eine neue Vermittlungsschichtadresse.

Der Kommunikationspfad

Sinn und Zweck der Vermittlungsschicht ist es, den besten Pfad durch das Netzwerk zu finden. Damit dies aber möglich ist, muss ein Netzwerk alle Pfade zwischen den Routern kennen. So besitzt jede Verbindung zwischen Routern eine Nummer, welche die Router als Netzadresse benutzen. Diese Adressen enthalten Informationen, die durch den Routing-Prozess zur Übermittlung von Paketen von einem Absender an einen Empfänger verwendet werden.



Transportnetze: Jede Verbindung zwischen Routern besitzt eine Nummer, welche die Router als Netzadresse benutzen.

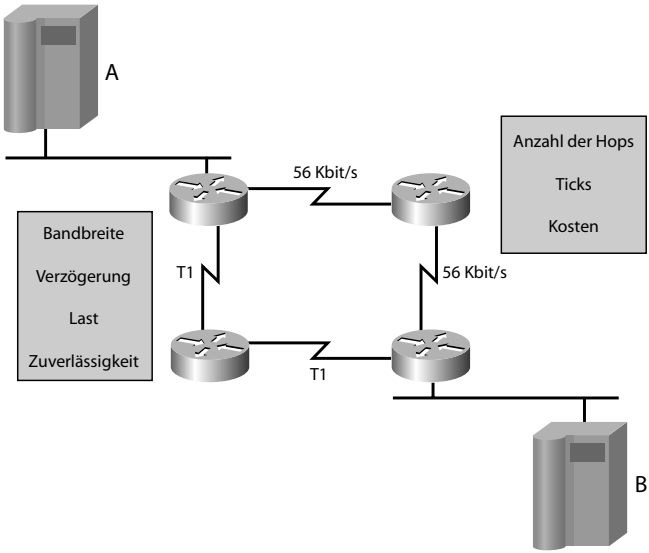
Mit diesen Adressen kann die Vermittlungsschicht eine Verbindung zwischen unabhängigen Netzwerken herstellen. Die Zusammenfassung von Schicht-3-Adressen in einem Router-Segment optimiert außerdem die Bandbreitennutzung, denn sie verhindert unnötige Broadcasts. Broadcasts verbrauchen Prozess- und Netzwerkkapazitäten, die anderweitig besser eingesetzt werden könnten, und belasten überdies Geräte und Verbindungen, die den jeweiligen Broadcast überhaupt nicht empfangen bzw. übertragen müssen. Wenn man eine konsistente Ende-zu-Ende-

Adressierung benutzt, dann kann die Vermittlungsschicht einen Pfad zum Empfänger ermitteln, ohne die Geräte oder Verbindungen im Netzwerk unnötig mit Broadcasts zu belasten.

1.1.12 Routing-Tabellen

Um den Vorgang der Pfadermittlung zu unterstützen, erstellen und führen Routing-Protokolle Routing-Tabellen, die Routendaten enthalten. Je nachdem, welches Routing-Protokoll verwendet wird, können die Routing-Informationen variieren. Routing-Protokolle tragen eine Vielzahl von Informationen in die Tabellen ein. Router halten eine Reihe wichtiger Informationen in den Routing-Tabellen auf dem aktuellen Stand. Zu diesen Informationen gehören die folgenden:

- Protokolltyp. Der Typ des Routing-Protokolls, das den Eintrag in der Routing-Tabelle erstellt hat.
- Verknüpfungen zwischen Empfängern und dem nächsten Hop. Diese Information sagt einem Router, dass ein bestimmter Empfänger entweder direkt an den Router angeschlossen ist, oder gibt einen anderen Router – den nächsten „Hop" – an, über den der Empfänger erreichbar ist. Wenn ein Router ein Paket erhält, überprüft er die Empfängeradresse und versucht, einen passenden Eintrag in der Routing-Tabelle zu finden.



Routing-Metriken: Routing-Algorithmen können ihre Routenauswahl auf mehrere Metriken beziehen, aus denen sie eine einzige, zusammengesetzte Metrik bilden.

- Routing-Metriken. Verschiedene Routing-Protokolle verwenden unterschiedliche Metriken. Diese Metriken erlauben, die Eignung einer Route festzulegen. Das RIP-Protokoll beispielsweise verwendet die Anzahl der Hops als Routing-Metrik, IGRP hingegen bildet aus Bandbreite, Last, Verzögerung und Zuverlässigkeit einen Metrikgesamtwert.
- Ausgangsport. Dies ist der Port, über den die Daten gesendet werden müssen, um zum gewünschten Empfänger zu gelangen.

Router kommunizieren miteinander, um ihre Routing-Tabellen auf einem aktuellen Stand zu halten, indem sie Routing-Updates austauschen. Je nach Routing-Protokoll werden diese Updates regelmäßig oder aber nur dann gesendet, wenn eine Änderung in der Netzwerktopologie stattgefunden hat. Das Routing-Protokoll bestimmt zudem, ob nur die geänderten Routen oder aber die gesamte Routing-Tabelle als Update gesendet wird. Durch Analyse der Routing-Updates, die von den benachbarten Routern kommen, kann ein Router seine eigene Routing-Tabelle erstellen und pflegen.

1.1.13 Routing-Algorithmen

Routing-Protokolle verfolgen häufig eines oder mehrere der folgenden Ziele:

- **Optimierung:** Dieser Begriff beschreibt die Fähigkeit eines Routing-Protokolls oder Algorithmus, unter Berücksichtigung von Metriken und ihrer Gewichtung die beste Route auszuwählen. Ein Algorithmus könnte etwa die Anzahl der Hops und die Verzögerung für die Metrik verwenden, der Verzögerung bei der Berechnung aber einen höheren Stellenwert zuweisen.
- **Einfachheit und geringe Belastung:** Im Idealfall wird die effiziente Funktionalität eines Routing-Algorithmus bei minimaler Belastung von Prozessor und Speicher erreicht. Dies ist wichtig, damit sich das Netzwerk auch in hohem Maße skalierbar bleibt (zum Beispiel das Internet).
- **Robustheit und Stabilität:** Ein Routing-Algorithmus sollte auch unter ungewöhnlichen oder nicht vorhersehbaren Umständen (Hardwareausfall, hohe Auslastung, Implementierungsfehler) einwandfrei funktionieren.
- **Schnelle Konvergenz:** Unter der Konvergenz versteht man einen Zustand, bei dem alle Router die gleichen (korrekten) Informationen zu allen Routen verwenden. Wenn ein Netzereignis Änderungen bei der Verfügbarkeit der Router hervorruft, werden Neuberechnungen notwendig, um die Verfügbarkeit der Netzwerkkonnektivität wiederherzustellen. Routing-Algorithmen, die langsam konvergieren, können einen Verlust von Daten verursachen.
- **Flexibilität:** Ein Routing-Algorithmus sollte sich schnell an eine Vielzahl von Änderungen im Netzwerk anpassen können. Zu diesen änderbaren Faktoren gehören die Verfügbarkeit der Router, geänderte Bandbreiten, Warteschlangenlänge und Verzögerungen im Netzwerk.

- **Skalierbarkeit:** Einige Routing-Protokolle sind besser für die Skalierung von Netzwerken geeignet als andere. Wenn Sie bereits von Anfang an wissen, dass ein Netzwerk wachsen wird (oder diese Möglichkeit in Betracht ziehen), dann sollten Sie etwa eher EIGRP als Routing-Protokoll verwenden als RIP.

Metriken

Wenn ein Routing-Algorithmus eine Routing-Tabelle aktualisiert, dann besteht sein primäres Ziel darin, die Pfadinformationen zu ermitteln, die für die Routing-Tabelle am geeignetsten sind. Dabei interpretiert jeder Routing-Algorithmus auf seine Weise, was als „das Geeignetste" zu betrachten ist. Für jeden Pfad durch das Netzwerk generiert der Algorithmus einen Wert, die so genannte Metrik. Anspruchsvolle Routing-Algorithmen können ihre Routenauswahl auf mehrere Metriken beziehen, aus denen sie eine einzige, zusammengesetzte Metrik bilden. Dabei ist ein Pfad umso besser, je geringer seine Metrik ist.

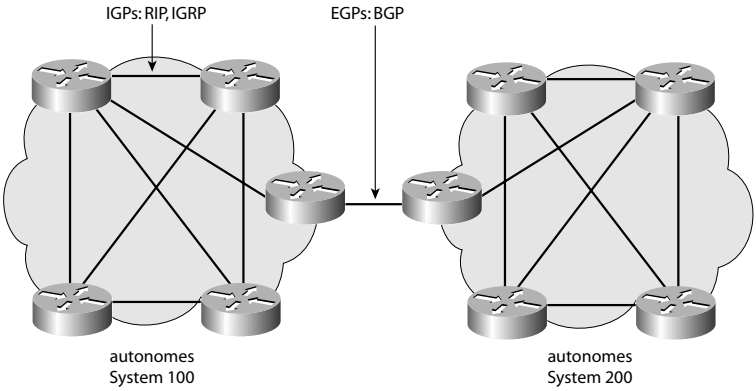
Metriken lassen sich sowohl auf der Basis eines einzelnen Merkmals als auch basierend auf mehreren Eigenschaften des Pfades errechnen. Zu den Metriken, die Routing-Protokolle am häufigsten verwenden, gehören die folgenden:

- **Bandbreite:** Die Datenkapazität einer Verbindung. Zum Beispiel ist eine Ethernet-Leitung mit 10 Mbit/s einer ISDN-Verbindung mit 64 Kbit/s vorzuziehen.
- **Verzögerung:** Die Zeit, die benötigt wird, um ein Paket über die jeweiligen Verbindungen vom Absender zum Empfänger zu übermitteln. Die Verzögerung hängt von verschiedenen Bedingungen ab: der Bandbreite der Zwischenverbindungen, den Port-Warteschlangen der einzelnen Router, der Netzwerkbelastung und der physischen Entfernung.
- **Last:** Umfang der Aktivitäten an einer Netzwerkressource (zum Beispiel an einem Router oder auf einer Leitung).
- **Zuverlässigkeit:** Bezeichnet die Fehlerrate der Netzwerkverbindung.
- **Anzahl der Hops:** Anzahl der Router, die ein Paket auf seinem Weg passieren muss, bevor es zum Empfänger gelangt. Wann immer Daten durch einen Router bewegt werden, spricht man von einem Hop. Wenn man von einem Pfad sagt, dass er vier Hops aufweise, dann müssen die Daten vom Absender kommend vier Router passieren, bevor sie beim Empfänger ankommen. Gibt es mehrere Pfade, wählt der Router den Pfad mit der geringsten Anzahl an Hops.
- **Kosten:** Ein frei einstellbarer Wert, der normalerweise auf der Bandbreite, finanziellen Aufwendungen und Ähnlichem basiert und vom Netzwerkadministrator zugewiesen wird.

1.1.14 Interne und externe Routing-Protokolle

Router benutzen Routing-Protokolle, um Routing-Informationen auszutauschen, das heißt, Routing-Protokolle bestimmen, wie geroutete Protokolle zu routen sind. Ein autonomes System ist ein Netzwerk oder ein Netzwerkverbund, der sich unter

der administrativen Kontrolle einer einzelnen Instanz befindet (zum Beispiel die Domäne cisco.com). Autonome Systeme bestehen aus Routern, die nach außen eine konsistente Routing-Ansicht zeigen.



IGP & EGP: Die Routing-Protokolle IGP (Interior Gateway Protocol) und EGP (Exterior Gateway Protocol) unterscheiden sich dadurch, wie sie in Bezug auf autonome Systeme verfahren.

Die IANA weist regionalen Registrierstellen Nummern zur Vergabe an autonome Systeme zu. Diese Registrierstellen sind die ARIN für Nord- und Südamerika sowie Afrika (Kontakt: hostmaster@arin.net), die RIPE-NCC in Europa (ncc@ripe.net) und die AP-NIC für den asiatischen und pazifischen Raum (admin@apnic.net). Bei den Nummern handelt es sich um 16-Bit-Zahlen. Ein Routing-Protokoll wie etwa BGP setzt voraus, dass Sie diese eindeutige, zugewiesene Nummer in Ihrer Konfiguration eintragen. IGP-Protokolle routen Daten innerhalb autonomer Systeme. Zu dieser Protokollfamilie gehören die folgenden Protokolle:

- RIP und RIPv2
- IGRP
- EIGRP
- OSPF
- ISIS (Intermediate System-to-Intermediate System)

EGP-Protokolle routen Daten zwischen autonomen Systemen. Der am weitesten verbreitete Vertreter der EGP-Protokolle ist BGP (Border Gateway Protocol).

1.1.15 Typen von Routing-Protokollen

Routing-Protokolle lassen sich auf viele unterschiedliche Arten – etwa als IGPs und EGPs – klassifizieren. Eine weitere Möglichkeit der Kategorisierung stellt die Unterscheidung in Distanzvektorprotokolle und Link-State-Protokolle dar. Wäh-

rend IGP und EGP die physischen Beziehungen von Routern beschreiben, zeigt die Klassifizierung in Distanzvektor- und Link-State-Protokolle, wie Router bezüglich Ihrer Routing-Updates miteinander kommunizieren.

Distanzvektor-Protokolle

Beim Distanzvektor-Routing werden für jede Verbindung im Netzwerkverbund eine Richtung (Vektor) und eine Distanz bestimmt. Distanzvektoralgorithmen senden regelmäßig (etwa alle 30 Sekunden) die Routing-Tabelle teilweise oder vollständig an ihre benachbarten Router. Router, die ein Distanzvektorprotokoll ausführen, senden diese regelmäßigen Updates auch dann, wenn keine Änderungen im Netzwerk aufgetreten sind. Wenn ein Router die Routing-Tabelle seines Nachbarn empfängt, kann er alle bekannten Routen überprüfen und bei Bedarf in der lokalen Routing-Tabelle Änderungen entsprechend den aktualisierten Informationen des benachbarten Routers vornehmen. Diesen Vorgang bezeichnet man als Routing by Rumor („gerüchtebasiertes Routing“), denn die Sichtweise eines Routers auf das Netzwerk basiert auf Perspektive, die sein Nachbar von der Netzwerktopologie hat. Distanzvektorprotokolle verwenden zur Ermittlung der optimalen Pfade den Bellman-Ford-Algorithmus.

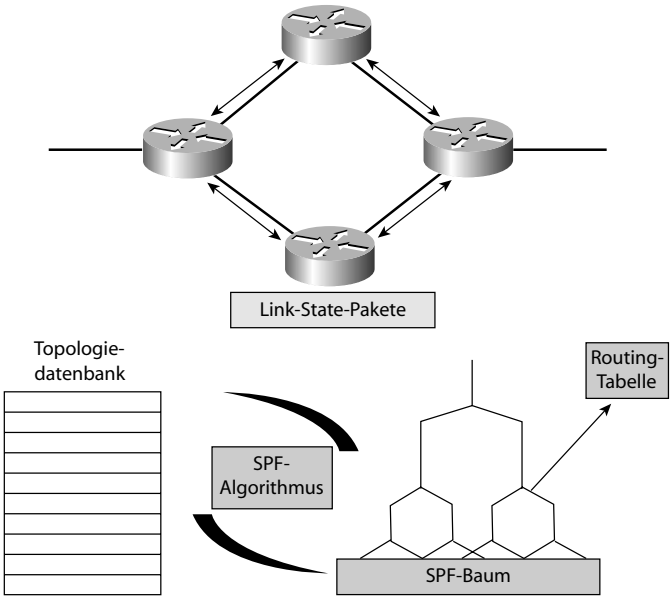
Die folgenden Protokolle gehören zu den Distanzvektorprotokollen:

- RIP (Routing Information Protocol). RIP ist das älteste und verbreiteste IGP im Netzwerk und verwendet die Anzahl der Hops als Metrik.
- IGRP (Interior Gateway Routing Protocol). Dieses IGP wurde von Cisco entwickelt, um Probleme in Zusammenhang mit dem Routing in größeren, heterogenen Netzwerken zu lösen.
- EIGRP (Enhanced Interior Gateway Routing Protocol). Hierbei handelt es sich um eine erweiterte Version von IGRP, die ebenfalls von Cisco entwickelt wurde. EIGRP bietet herausragende Konvergenzeigenschaften und ermöglicht einen effizienten Betrieb, indem es die Vorzüge von den Link-State- und den Distanzvektorprotokollen vereinigt.

Link-State-Protokolle

Link-State-Protokolle wurden entwickelt, um die durch Distanzvektorprotokolle auferlegten Beschränkungen zu umgehen. Sie reagieren schnell auf Änderungen im Netzwerk, senden Trigger-Updates nur dann, wenn die Netzwerktopologie tatsächlich geändert wurde, und periodische Updates – so genannte Refreshs – in langen Zeitabständen (alle 30 Minuten).

Wenn eine Verbindung ihren Status ändert, erstellt das Gerät, das diese Änderung erkannt hat, ein LSA (Link-State-Advertisement, Anzeige des Routenstatus) zu einer Route, und dieses LSA wird dann an alle benachbarten Geräte übermittelt. Jedes Routing-Gerät aktualisiert anhand des LSA die Topologiedatenbank und leitet es danach an alle Nachbarn weiter. Dieses Fluten des LSA ist notwendig, um sicherzustellen, dass alle Routing-Geräte ihre Datenbanken aktualisieren, bevor sie eine aktuelle Routing-Tabelle erstellen, welche die neue Topologie berücksichtigt.



Optimierung: Link-State-Router finden durch den SPF-Algorithmus (Shortest Path First) den optimalen Pfad durch das Netzwerk.

Die Link-State-Datenbank dient als Grundlage zur Berechnung der optimalen Pfade durch das Netzwerk. Link-State-Router finden diese Pfade durch Anwendung des SPF-Algorithmus (Shortest Path First) auf die Link-State-Datenbank, um so einen SPF-Baum zu erstellen. Die besten (kürzesten) Pfade werden dann aus dem SPF-Baum ausgewählt und in der Routing-Tabelle abgelegt. Zu den Link-State-Protokollen gehören OSPF und IS-IS.

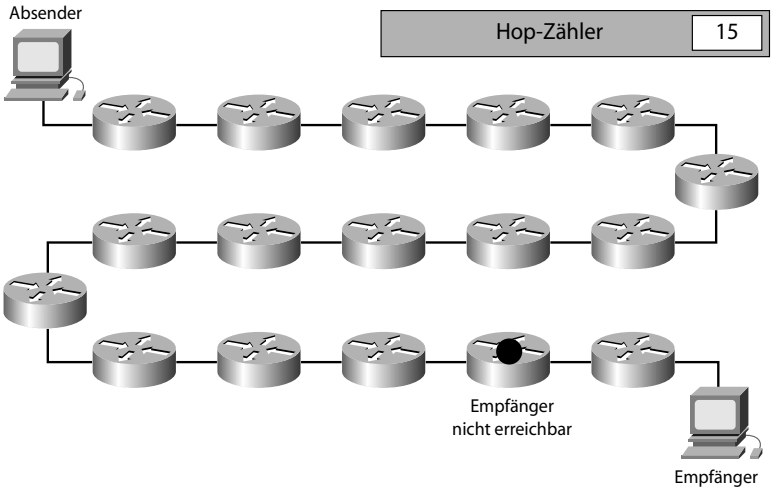
Eigenschaften von Routing-Protokollen

Die nachfolgend beschriebenen meistverwendeten Routing-Protokolle unterscheiden sich in den Metriken, Einsatzbereiche und anderen wichtige Merkmalen.

RIP (Routing Information Protocol)

RIP verwendet die Anzahl der Hops zur Ermittlung von Richtung und Länge der Verbindungen im Netzwerk. Wenn mehrere Pfade zum Ziel vorhanden sind, wählt RIP denjenigen mit den wenigsten Hops. Da allerdings die Anzahl der Hops die einzige von RIP verwendete Metrik ist, wird hierbei nicht unbedingt der schnellste Pfad zum Empfänger gewählt. RIPv1 verwendet nur klassenorientiertes Routing, d.h., alle Geräte im Netzwerk müssen die gleiche Subnetzmaske benutzen, weil RIPv1 keine Subnetzinformationen mit dem Routing-Update übermittelt. RIPv2 hingegen bietet so genanntes Präfix-Routing und sendet Subnetzdaten mit den

Routing-Updates, unterstützt also die Verwendung klassenlosen Routings. Bei klassenlosen Routing-Protokollen können unterschiedliche Subnetze innerhalb eines Netzwerks auch unterschiedliche Subnetzmasken haben. Die Verwendung verschiedener Subnetzmasken innerhalb eines einzigen Netzwerks nennt man VLSM (Variable Length Subnet Masking).



RIP: Das Protokoll verwendet die Anzahl der Hops als Routing-Metrik.

IGRP (Interior Gateway Routing Protocol)

IGRP ist ein Distanzvektorprotokoll, das von Cisco entwickelt wurde, um Probleme in Zusammenhang mit dem Routing in größeren Netzwerken zu lösen, die andere Protokolle wie etwa RIP überfordern. IGRP wählt den schnellsten Pfad basierend auf der Verzögerung, der Bandbreite, der Last und der Zuverlässigkeit. Standardmäßig verwendet IGRP nur die Bandbreite und die Verzögerung als 24-Bit-Metriken. Ferner hat IGRP eine wesentlich höhere Obergrenze für die Anzahl der Hops als RIP, erlaubt also eine bessere Skalierung des Netzwerks. IGRP verwendet nur klassenorientiertes Routing.

EIGRP (Enhanced Interior Gateway Routing Protocol)

Wie IGRP ist auch EIGRP ein proprietäres Cisco-Protokoll. Es handelt sich um eine fortgeschrittene IGRP-Version mit 32-Bit-Metrik. Im Wesentlichen bietet EIGRP ein überlegenes Betriebsverhalten durch schnellere Konvergenz und einen geringeren Bandbreitenbedarf für Steuerdaten. EIGRP ist ein fortschrittliches Distanzvektorprotokoll und verwendet auch einige Funktionen, die man von Link-State-Protokollen kennt. Insofern wird EIGRP auch als Hybridprotokoll bezeichnet.

OSPF (Open Shortest Path First)

OSPF ist ein Link-State-Protokoll, das von der IETF (Internet Engineering Task Force) 1988 entwickelt wurde, um die Anforderungen sehr großer, skalierbarer Netzwerke zu erfüllen, die RIP überforderten. Die aktuelle Version OSPFv2 wird in RFC 2328 beschrieben. OSPF ist ein IGP, das heißt, es verbreitet Routing-Informationen unter Routern, die zum gleichen autonomen System gehören.

IS-IS (Intermediate System-to-Intermediate System)

IS-IS ist das dynamische Link-State-Protokoll für den OSI-Protokollstapel. Als solches verteilt es Informationen für das Routing von CLNP-Daten (Connectionless Network Protocol) in ISO-kompatiblen CLNS-Umgebungen (Connectionless Network Service). Integriertes IS-IS ist eine Implementierung dieses Protokolls für das gemeinsame Routing mehrerer Netzwerkprotokolle. Diese Variante kann CLNP-Routen mit Informationen zu IP-Netzwerken und Subnetzen kennzeichnen und stellt in der IP-Welt eine Alternative zu OSPF dar, weil es gemischtes CLNS- und IP-Routing innerhalb eines Protokolls ermöglicht: Integriertes IS-IS kann sowohl für reines IP-Routing als auch für reines ISO-Routing oder eine Mischung der beiden verwendet werden.

BGP (Border Gateway Protocol)

BGP ist ein EGP-Protokoll. Es tauscht Routing-Informationen zwischen autonomen Systemen aus und garantiert gleichzeitig eine schleifenfreie Pfadauswahl. BGP ist das von großen Firmen und Internetprovidern meistverwendete Protokoll zur Bekanntgabe von Routen im Internet. BGP4 ist die erste BGP-Version, die CIDR (Classless Interdomain Routing, klassenloses domänenübergreifendes Routing) und Routen-Aggregation (Zusammenfassung mehrerer Routen) unterstützt. Anders als andere IGPs wie RIP, OSPF und EIGRP verwendet BGP keine Metriken wie Anzahl der Hops, Bandbreite oder Verzögerung, sondern trifft seine Entscheidungen basierend auf Richtlinien oder Regeln im Netzwerk, wobei verschiedene BGP-Pfadattribute zum Einsatz kommen.

1.1.16 Grundlagen der Subnetzbildung

Die Subnetzbildung trennt vorhandene Netzwerke in einzelne Segmente. Dadurch verringert sich die Domänen-Größe, die Sicherheit in LAN-Segmenten erhöht sich. Die ursprünglich zweistufige Hierarchie des Internets ging davon aus, dass an jedem Standort nur ein einziges Netzwerk vorhanden ist, weswegen alle Standorte nur jeweils eine Internetverbindung benötigten. Im Laufe der Zeit jedoch stimmte diese Voraussetzung nicht mehr, denn die Netzwerktechno¬logie wuchs und reifte, und bereits im Jahre 1985 war es keineswegs mehr sicher, dass eine Organisation sich auf ein einziges Netzwerk beschränkte oder sich mit einer einzelnen Internetverbindung zufrieden gab.

Als damit begonnen wurde, an einem Standort mehrere Netzwerke zu implementieren, stellte man bei der IETF bald fest, dass eine Methode benötigt wurde, mit der sich zwischen den vielen logischen Netzwerken unterscheiden ließ, die als Untergruppen der zweiten Internetebene entstanden waren. Ohne einen solchen Mechanismus gäbe es keine Möglichkeit, Daten effizient zu bestimmten Endsystemen an Standorten mit mehreren Netzwerken zu routen.

1.1.17 IP-Adressklassen

Die verschiedenen IP-Adressklassen verfügen über jeweils zwischen 256 und 16,8 Millionen Adressen. Um die begrenzte Anzahl an IP-Adressen verwalten zu können, lassen sich alle Klassen in kleinere Subnetze unterteilen.

Unterteilung: Netz- und Hostanteile bei den IP-Adressen der Klassen A, B, C und D.

Klasse A	Netzwerk	Host		
Oktett	1	2	3	4

Klasse B	Netzwerk		Host	
Oktett	1	2	3	4

Klasse C	Netzwerk			Host
Oktett	1	2	3	4

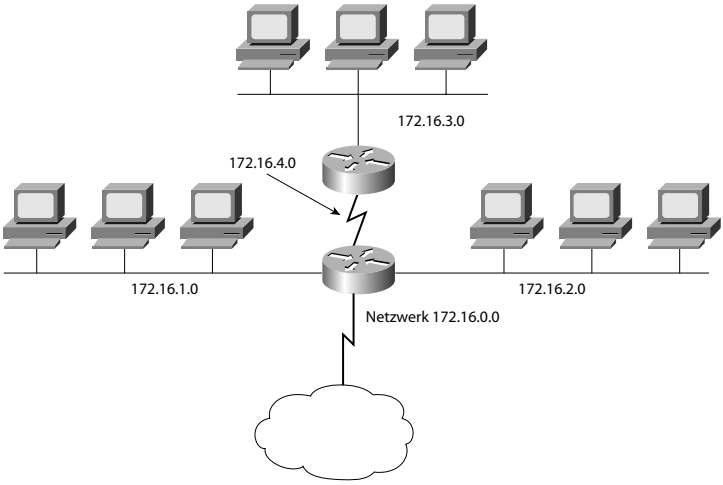
Klasse D	Host			
Oktett	1	2	3	4

1.1.18 Subnetzbildung – Basics

Damit eine Subnetzstruktur gebildet werden kann, müssen Hostbits als Netzwerkbits definiert werden, indem das Hostoktett beziehungsweise die Hostoktette unterteilt werden. Man bezeichnet dies als „Borgen“ von Bits.

Der Ausgangspunkt dieses Vorgangs ist immer das ganz links stehende Hostbit – welches dies ist, hängt von der IP-Klasse ab. Die Subnetzbildung erleichtert nicht nur die Verwaltung von Netzwerken, sondern erlaubt dem Netzwerkadministrator auch eine Begrenzung von Broadcasts und bietet LAN-Sicherheit auf niedriger

Ebene. Sicherer wird ein LAN durch Subnetzbildung, weil der Zugriff auf andere Subnetze über einen Router erfolgt. Der Router kann so konfiguriert werden, dass er den Zugriff auf ein Subnetz basierend auf verschiedene Kriterien zulässt oder verweigert. Außerdem haben einige Besitzer von Klasse-A- und Klasse-B-Netzwerken entdeckt, dass die Subnetzbildung ihnen eine neue Einnahmequelle verschafft: Sie verkaufen oder vermieten heute nicht benötigte IP-Adressen.



Subnetze: In einer Umgebung mit mehreren Netzwerken ist jedes Subnetz über einen gemeinsamen Punkt – den Router – mit dem Internet verbunden.

Wie die interne Netzwerkumgebung genau aussieht, ist für das Internet nicht von Belang. Die Erreichbarkeit des eigenen Netzwerks wird dem Internet weltweit mit den Datagrammen des EGP-Protokolls bekannt gemacht.

Aus diesem Grund muss das Internet nur wissen, wie es den Gateway-Router – also den Anbindungspunkt des Netzwerks an das Internet – erreichen kann. Innerhalb des privaten Netzwerks kann der Hostanteil der IP-Adresse jedoch zur Bildung von Subnetzen verwendet werden.

Da die Subnetzadresse dem Hostanteil der Klasse-A-, Klasse-B- und Klasse-C-Adressen entnommen wird, kann sie lokal zugewiesen werden. Dies erledigt in der Regel der Netzwerkadministrator. Natürlich müssen, wie die anderen Teile von IP-Adressen, auch die Subnetzadressen innerhalb des Bereichs eindeutig sein.

Subnetze fügen LANs zu einem WAN

Die Subnetzbildung wird häufig benötigt, wenn LANs zu einem WAN zusammengeschlossen werden. Wenn Sie beispielsweise zwei LANs miteinander verbinden wollen, die geografisch weit voneinander entfernt sind, dann sind in der Regel die-

se LANs und das sie verbindende WAN jeweils als eigenes Subnetz zu konfigurieren. Für diesen Zweck benötigen Sie zwei Router (einer in jedem LAN), um Pakete zwischen den LANs auszutauschen.

Ein weiterer wesentlicher Grund für die Verwendung von Subnetzen ist die Verkleinerung einer Broadcast-Domäne. Broadcasts werden an alle Hosts in einem Netzwerk oder Subnetz gesendet. Wenn aufgrund des Versands von Broadcasts die Bandbreite spürbar verringert wird, dann sollte jeder Netzwerkadministrator über eine Verkleinerung seiner Broadcast-Domäne nachdenken.

Nach außen präsentiert sich ein LAN als einzelnes Netzwerk, ohne dass die internen Netzwerkstrukturen offenbar werden. Diese Sichtweise des Netzwerks sorgt dafür, dass Routing-Tabellen klein und überschaubar bleiben. Von der lokalen Knotenadresse 192.168.10.14 ist nach außen hin nur die Netzwerkadresse 192.168.10.0 sichtbar; Grund hierfür ist, dass die Adresse 192.168.10.14 nur innerhalb des LAN 192.168.10.0 gültig ist; außerhalb kann sie nicht verwendet werden.

Subnetzadressen setzen sich aus dem Netzanteil der Klasse-A-, Klasse-B- bzw. Klasse-C-Adresse, einem Subnetzfeld und einem Hostfeld zusammen. Subnetzfeld und Hostfeld werden dabei aus dem ursprünglichen Hostanteil des Gesamtnetzwerks erstellt. Die Möglichkeit zu entscheiden, wie der ursprüngliche Hostanteil in diese beiden neuen Felder unterteilt wird, macht die Adressierung für den Netzwerkadministrator erheblich flexibler. Das bedeutet nichts anderes, als dass der Administrator sowohl bei der ursprünglichen Erstellung des Adressschemas als auch bei einer späteren Erweiterung des Netzwerkes mehr Möglichkeiten hat.

1.1.19 Subnetzmaske erstellen

Die Auswahl der Anzahl der Bits für den Subnetzanteil hängt von der maximalen Anzahl der Hosts pro Subnetz ab. Um eine Konfiguration von Subnetzen vornehmen zu können, müssen Sie die Grundlagen der binären Mathematik beherrschen und den Positionswert der Bits in den einzelnen Oktetten kennen.

Bitpositionen und -werte für die Subnetzbildung								
Bit	1	2	3	4	5	6	7	8
Wert	128	64	32	16	8	4	2	1

Unabhängig von der IP-Adressklasse können allerdings die letzten beiden Bits des letzten Oktetts keinem Subnetz zugewiesen werden. Wenn Sie alle verfügbaren Bits bis auf diese beiden als Subnetzanteil verwenden, können sie genau zwei Hosts pro Subnetz ansprechen. Diese Methode wird häufig zum Einsparen von Adressen bei der Adressvergabe für serielle Router-Verbindungen verwendet; in einem funktionsfähigen LAN jedoch würde dieses Verfahren die Hardware-Kosten auf ein untragbares Maß erhöhen.

Um eine Subnetzmaske zu erstellen, die dem Router genug Informationen zur Zuordnung eines Hosts zu einem bestimmten Subnetz gibt, wählen Sie die Spalte mit der Anzahl der Bits aus, und ermitteln Sie dann die zugehörige Maskennummer. Diese Nummer wird berechnet, indem der Positionswert der verwendeten Bits hinzuaddiert wird. Wenn also drei Bits verwendet würden, dann lautete die Maske einer Klasse-C-Adresse 255.255.255.224 (siehe nachfolgende Tabelle). Diese Maske kann auch als Zahl hinter einem Schrägstrich angegeben werden – hier also /27. Die auf den Schrägstrich folgende Zahl ist die Gesamtzahl der Bits in Netzwerkanteil und Subnetzmaske.

Subnetzmaskenbezeichnung (zwei Formate)								
Schrägstrichformat	/25	/26	/27	/28	/29	/30	–	–
Maske	128	192	224	240	248	252	254	255
Bit	1	2	3	4	5	6	7	8
Wert	128	64	32	16	8	4	2	1

Bit-Bestimmung bei Subnetzen

Um die Anzahl der Bits zu bestimmen, die verwendet werden können, muss der Netzdesigner festlegen, wie viele Hosts im größten Subnetz zum Einsatz kommen sollen und wie viele Subnetze gebildet werden sollen. Nehmen wir zum Beispiel einmal an, dass fünf Subnetze mit jeweils maximal 30 Hosts eingerichtet werden sollen. Um nun zu ermitteln, wie viele Bits neu zugewiesen wer¬den müssen, verwenden Sie die Zeile „Hosts (max.)“ in der Tabelle.

Subnetze und Hosts								
Schrägstrichformat	/25	/26	/27	/28	/29	/30	–	–
Maske	128	192	224	240	248	252	254	255
Bit	1	2	3	4	5	6	7	8
Wert	128	64	32	16	8	4	2	1
Subnetzadressen (ges.)		4	8	16	32	64		
Subnetze (max.)		2	6	14	30	62		
Hostadressen (ges.)		64	32	16	8	4		
Hosts (max.)		62	30	14	6	2		

Für die 30 Hosts werden drei Subnetzbits benötigt. Hierdurch werden sechs Subnetze realisiert, was die Anforderungen in unserem Beispiel ebenfalls erfüllt. Auch hier ist die Differenz zwischen den maximal verwendbaren Subnetzen und der Gesamtanzahl der Subnetze die Folge der Verwendung der ersten verfügbaren Subnetzadresse als Netzwerkkennung und der letzten Adresse als Broadcast-Adresse für alle Subnetze. Das klassenorientierte Routing bietet keine Möglichkeit zur Nutzung dieser Subnetze, während das klassenlose Routing viele dieser „verlorenen" Adressen wiederherstellt. Die Tabelle veranschaulicht den Verlust an Subnetzen und Hosts bei Verwendung eines klassenorientierten Protokolls.

Eine andere Möglichkeit, die Subnetzmaske und die Anzahl der Netzwerke zu berechnen, besteht in der Verwendung der nachfolgend beschriebenen Formeln. Die erste Formel besagt, dass die maximale Anzahl der Subnetze der Differenz von 2 zur Potenz der zugewiesenen Subnetzbits und 2 entspricht:

$2^{(\text{Anzahl der zugewiesenen Bits})} - 2 = \text{maximale Anzahl der Subnetze}$

Beispiel: $2^3 - 2 = 6$

Die zweite Formel besagt, dass die maximale Anzahl der Hosts der Differenz von 2 zur Potenz der verbleibenden Bits und 2 entspricht:

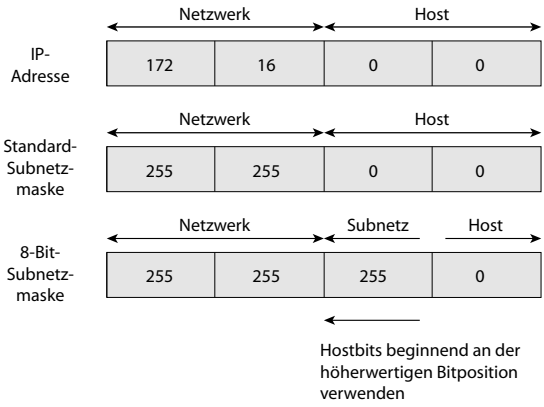
$2^{(\text{Anzahl der verbleibenden Bits})} - 2 = \text{maximale Anzahl der Hosts}$

Beispiel: $2^5 - 2 = 30$

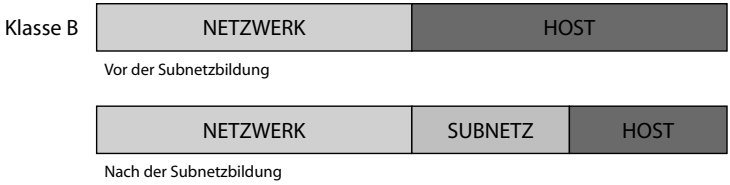
1.1.20 Subnetzmaske anwenden

Um Subnetze bilden zu können, muss man den Routing-Anteil der Adresse erweitern. Das Internet „kennt" ihr Netzwerk nur als Ganzes, das heißt, es sieht Klasse-A-, Klasse-B- oder Klasse-C-Adressen und bezieht daraus dann die Anzahl der Routing-Bits (8, 16 oder 24).

Gleiches Prinzip: Subnetzmasken nuten das Gleiche Format wie IP-Adressen.



Im Subnetzfeld befinden sich weitere Routing-Bits, so dass auch Ihre organisationsinternen Router Standorte und Subnetze in Ihrem Gesamtnetzwerk unterscheiden können. Subnetzmasken verwenden das gleiche Format wie IP-Adressen. Beide haben eine Länge von 32 Bit und sind in vier Oktette unterteilt. Bei Subnetzmasken besteht der Netz- und Subnetzanteil ausschließlich aus Einsen, der Hostanteil aus Nullen. Werden keine Bits geborgt, dann ist beispielsweise die Standardsubnetzmaske für Klasse-B-Netzwerke als 255.255.0.0 definiert. Werden bei einem solchen Netzwerk jedoch acht Bits für die Subnetzadresse benötigt, dann lautet die Subnetzadresse für das Netzwerk 255.255.255.0. Da zwei Oktette für das Hostfeld eines Klasse-B-Netzwerks vorgesehen sind, lassen sich bis zu 14 Bits für die Bil¬dung von Subnetzen verwenden. Im Gegensatz dazu ist für Klasse-C-Netzwerke nur ein Oktett als Hostanteil definiert, weswegen sich nur sechs Bits für die Subnetzbildung nutzen lassen.



B-Klasse: Das Subnetzfeld folgt immer unmittelbar auf den Netzanteil. Die geliehenen Bits für das Subnetz müssen die ersten n Bits des Hostanteils sein. Die Subnetzmaske ist das Werkzeug, mit dem der Router feststellen kann, welche Bits Routing-Bits und welche Hostbits sind.

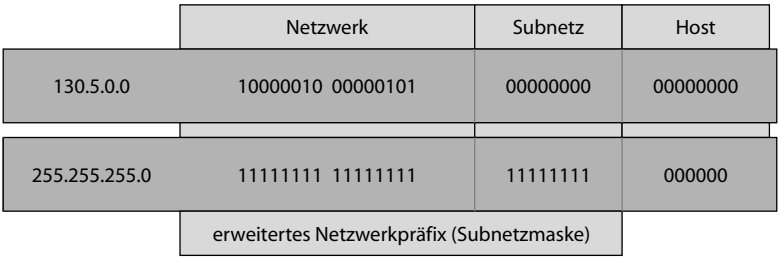
1.1.21 Größe der Subnetzmaske bestimmen

Wie bereits gesagt, enthält die Subnetzmaske an den Netzanteilposition (entsprechend der Adressklasse) und Subnetzanteilpositionen nur Einsen und an den verbleibenden Positionen nur Nullen, das heißt, diese Nullbits bilden den Hostanteil der Adresse. Standardmäßig wäre die Subnetzmaske eines Klasse-B-Netzwerks 255.255.0.0, wenn keine Bits für die Subnetzbildung geliehen würden; diese Maske entspräche einem 16 Bit langen, nur aus Einsen bestehenden Netzwerkanteil und einer ebenso langen, nur aus Nullen bestehenden Host-ID.

Würden nun acht Bits für das Subnetzfeld definiert werden, dann würde die Subnetzmaske acht zusätzliche Einserbits enthalten und 255.255.255.0 lauten. Wenn diese Subnetzmaske 255.255.255.0 mit der Klasse-B-Adresse 130.5.2.144 verknüpft würde, dann würde der Router wissen, dass er ein Paket nicht an das Netzwerk 130.5.0.0, sondern an das Netzwerk 130.5.2.0 weiterleiten müsste.

Noch ein Beispiel: Angenommen, ein Host hätte die Adresse 197.15.22.131, das zugehörige Klasse-C-Netzwerk die Subnetzmaske 255.255.255.224. Der Wert 224 im letzten Oktett (binär 11100000) zeigt an, dass der 24 Bit lange Netzanteil der Adresse um weitere drei Bits für Subnetze erweitert wurde, insgesamt also 27

Bits umfasst. Die 131 im letzten Oktett unserer Hostadresse zeigt, an, dass dies die dritte verwendbare Adresse im Subnetz 197.15.22.128 ist. Die Internet-Router (welche die Subnetzmaske nicht kennen) müssen die Daten lediglich an das Klasse-C-Netzwerk 197.15.22.0 weiterleiten; die verbleibende Weiterleitung übernehmen die netzwerkinternen Router, denn sie kennen die Subnetzmaske und berücksichtigen deswegen bei der Routing-Entscheidung 27 Bits.



Verknüpfung: Subnetzmaskierung einer Klasse-B-Adresse.

Subnetzmaske und IP-Adresse berechnen

Wenn Sie Bits des Hostanteils borgen, dann ist es wichtig, die Anzahl zusätzlicher Subnetze zu vermerken, die dadurch geschaffen werden, dass Sie ein oder mehrere Bits leihen. Sie wissen bereits, dass Sie mindestens zwei Bits leihen müssen; mit nur einem Bit lässt sich nichts anfangen.

Mit zwei Bits lassen sich vier Subnetze bilden (2 × 2), aber Sie müssen beachten, dass zwei der vier Adressen reserviert beziehungsweise nicht zu verwenden sind. Jedes Mal, wenn Sie ein weiteres Bit aus der Host-ID borgen, verdoppelt sich die Anzahl der erstellbaren Subnetze. Borgen Sie also drei Bits, dann können Sie acht Subnetze bilden (2 × 2 × 2), bei vier Bits sind es bereits 16 Subnetze (2 × 2 × 2 × 2). Aus diesen Beispielen ist ersichtlich, dass die Anzahl der möglichen Subnetze sich mit jedem aus dem Hostanteil geborgten Bit verdoppelt.

Jedes Mal, wenn Sie ein Bit des Hostanteils für die Subnetzbildung entleihen, bleibt für die Adressierung der Hosts ein Bit weniger übrig. Daraus ergibt sich, dass sich die Anzahl möglicher Hosts beim Entleihen eines Bits halbiert.

Damit Sie besser verstehen, wie das funktioniert, wollen wir es an einer Beispieladresse der Klasse C demonstrieren. Wenn es keine Subnetzmaske gibt, dann werden alle acht Bits des letzten Oktetts für den Hostanteil verwendet. Daraus ergibt sich eine Anzahl von $2^8 = 256$ möglichen Adressen (von denen 254 nach Abzug der beiden nicht verwendbaren Adressen übrig bleiben). Stellen wir uns nun einmal vor, dass dieses Klasse-C-Netzwerk in Subnetze gegliedert wird. Wenn Sie nun zwei der acht Bits des Hostanteils borgen, dann ist der Hostanteil nur noch sechs Bits lang. Daraus ergibt sich eine mögliche Anzahl von $2^6 – 2 = 62$ adressierbaren Hosts. Würde man drei Bits für die Subnetzbildung verwenden, dann blie-

ben $2^5 - 2 = 30$ Adressen. Die Anzahl der in einem Subnetz verwendbaren Hostadressen hängt also direkt von der Anzahl der gebildeten Subnetze ab. In einem Klasse-C-Netzwerk mit der Subnetzmaske 255.255.255.224 beispielsweise würden drei Bits für die Subnetzbildung benutzt (das Binäräquivalent der Dezimalzahl 224 heißt 11100000), fünf Bits verblieben für die Hostadressierung. Es lassen sich also auf diese Weise $8 - 2 = 6$ einsetzbare Subnetze mit jeweils $32 - 2 = 30$ verwendbaren Hostadressen bilden.

1.1.22 Subnetze in Klasse-A- und Klasse-B-Netzwerken bilden

Die Vorgehensweise zur Subnetzbildung bei Klasse-A- und Klasse-B-Adressen ist mit der bei Klasse-C-Adressen identisch, nur müssen hier gegebenenfalls deutlich mehr Bits berücksichtigt werden. 22 Bits stehen für das Subnetzfeld in Klasse-A-Adressen zur Verfügung, 14 Bits bei Klasse-B-Adressen.

Klasse-B-Netzadresse 147.10.0.0 (14 Bits verfügbar)
11001011.00001010. 00000000.00000000 N . N . H . H
10010011.00001010. 00000000 .00000 000 N . N . sN . sN H In diesem Beispiel wurden 12 Bits zur Bezeichnung des Subnetzes verwendet.

14 Bits verfügbar: Hostbits einer Klasse-B-Adresse leihen.

Klasse-A-Netzwerkadresse 28.0.0.0 (22 Bits verfügbar)
00011100. 00000000.00000000.00000000 N . H . H . H
00011100. 00000000 .00000000 .0000 0000 N . sN . sN . sN H In diesem Beispiel wurden 20 Bits zur Bezeichnung des Subnetzes verwendet.

22 Bits verfügbar: Hostbits einer Klasse-A-Adresse leihen.

Weist man zwölf Bits einer Klasse-B-Adresse dem Subnetzfeld zu, so entsteht die Subnetzmaske 255.255.255.240 (oder /28). Alle acht Bits des dritten und vier Bits des vierten Oktetts wurden als Subnetzfeld deklariert, das heißt, in der Subnetzmaske heißen die letzten beiden Oktette 255.240. Die Notierung der Subnetzmaske mit Schrägstrich nennt die Summe aller Netzwerk- und Subnetzbits.

Weist man nun bei einer Klasse-A-Adresse dem Subnetzfeld 20 Bits zu, dann entsteht ebenfalls die Subnetzmaske 255.255.255.240 (oder /28). In dieser Situation sind die Subnetzmasken der Klassen A und B identisch: Wird die Maske also nicht mit einer Netzwerkadresse verknüpft, dann ist es nicht möglich zu sagen, wie viele Bits zum Subnetzfeld gehören. Die folgenden Regeln gelten unabhängig davon, in welcher Adressklasse Subnetze gebildet werden:

$2^{(\text{Anzahl der zugewiesenen Bits})} = \text{Gesamtanzahl der Subnetze}$

$2^{(\text{Anzahl der verbleibenden Bits})} = \text{Gesamtanzahl der Hosts}$

$2^{(\text{Anzahl der zugewiesenen Bits})} - 2 = \text{maximale Anzahl der Subnetze}$

$2^{(\text{Anzahl der verbleibenden Bits})} - 2 = \text{maximale Anzahl der Hosts}$

1.1.23 Netzadresse mit booleschem UND berechnen

Wie bereits mehrfach angemerkt, besteht der Hostanteil bei den Netzwerk- oder Subnetzadressen immer aus Nullen. Damit ein Router ein Datenpaket weiterleiten kann, muss er zunächst die Adresse des Empfängernetzwerks oder Empfängersubnetzes ermitteln. Hierzu verknüpft er die IP-Adresse des Zielhosts und die Subnetzmaske mithilfe einer logischen UND-Operation.

Nehmen wir einmal an, Sie haben ein Klasse-B-Netzwerk mit der Netzwerkadresse 172.16.0.0. Nachdem Sie Ihr Netzwerk überprüft haben, kommen Sie zu dem Schluss, dass Sie acht Bits leihen müssen, um Subnetze zu bilden. Wie wir bereits wissen, heißt, wenn Sie in einem Klasse-B-Netzwerk acht Bits leihen, die Subnetzmaske 255.255.255.0. Jemand sendet nun von außerhalb Daten an die IP-Adresse 172.16.2.120. Damit der Router weiß, wohin die Daten zu leiten sind, verknüpft er diese Adresse über ein boolesches UND mit der Subnetzmaske.

Wenn diese beiden Nummern nun mit Hilfe der UND-Operation verknüpft werden, bleibt der Hostanteil immer 0. Was dann übrig bleibt, ist der Netzanteil einschließlich des Subnetzanteils. Die Daten werden also an das Subnetz 172.16.2.0 geschickt, und nur der letzte Router stellt fest, dass das Paket an den Host mit der Nummer 120 adressiert ist.

	Netzwerk	Subnetz	Host
IP-Hostadresse 172.16.2.120	10101100 00010000	00000010	01111000
Subnetzmaske 255.255.255.0 oder /24	11111111 11111111	11111111	00000000
Subnetz	10101100 00010000 172 16	00000010 2	00000000 0

Boolesche Verknüpfung: Acht Bits zur Subnetzbildung leihen.

Stellen Sie sich nun vor, dass Sie in unserem Beispielnetzwerk 172.16.0.0 nicht acht, sondern nur sieben Bits für das Subnetzfeld zuweisen. Die binäre Subnetzmaske lautete also 11111111.11111111.11111110.00000000. Wie sähe die Subnetzmaske in Dezimalnotation aus?

Wiederum sendet nun jemand von außerhalb des Netzwerks Daten an den Host 172.16.2.120. Auch hier verknüpft der Router die IP-Adresse und Subnetzmaske mithilfe der UND-Funktion, und auch jetzt besteht der Hostanteil nur aus Nullen. Wo also liegt der Unterschied zum ersten Beispiel. Alles sieht gleich aus – zumindest auf der dezimalen Ebene. Der Unterschied besteht in der Anzahl der vorhandenen Subnetze und der pro Subnetz verfügbaren Hostadressen. Diesen Unterschied stellt man aber nur beim Vergleich der beiden unterschiedlichen Subnetzmasken fest. Wenn der Subnetzanteil nur aus sieben Bits besteht, dann kann es nur 126 Subnetze geben. Wie viele Host lassen sich so pro Subnetz adressieren? Wie lang ist das Hostfeld? Antwort: Mit neun Bits als Hostanteil lassen sich in jedem der 126 Subnetze 510 Hosts ansprechen.

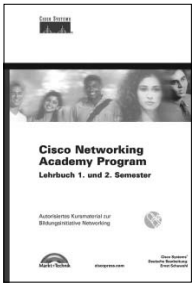
1.1.24 Fazit

Wenn die Daten im Netzwerk übertragen werden, benötigen die Netzwerkgeräte eine Möglichkeit zu erkennen, welcher Anteil der IP-Adresse das Netzwerk und welcher den Host bezeichnet. Hier kommt eine 32-Bits-Adressmaske – die Subnetzmaske – zum Einsatz, die angibt, welche Bits einer IP-Adresse als Netzwerkadresse verwendet werden. Die Standardmaske einer Klasse-A-Adresse ist 255.0.0.0, die einer Klasse-B-Adresse 255.255.0.0 und die einer Klasse-C-Adresse 255.255.255.0. Mithilfe der Subnetzmaske lassen sich vorhandene Netzwerke in Subnetze unterteilen.

Die Subnetzbildung verringert die Größe von Broadcast-Domänen, ermöglicht LAN-Segmenten an verschiedenen geografischen Standorten die Kommunikation über Router und bietet mehr Sicherheit und Trennung der einzelnen LAN-Segmente. Benutzerdefinierte Subnetzmasken verwenden mehr Bits als die Standardnetzwerkmasken. Diese zusätzlichen Bits werden vom Hostanteil der IP-Adresse geborgt. Hierdurch lässt sich eine IP-Adresse in die ursprüngliche Netzwerkadresse, der aus den geborgten Bits bestehende Subnetzadresse sowie die aus den verbleibenden Bits bestehende Hostadresse dreiteilen.

Router verwenden Subnetzmasken, um den Subnetzanteil der Adresse eines eingehenden Pakets zu bestimmen. Für diesen Prozess verwenden Router eine logische UND-Verknüpfung. (cvi)

Weiterführende Infos



Die Artikelserie „Grundlagen zu Routing und Subnetzbildung“ basiert auf dem Kapitel 10 des Standardwerks „Cisco Networking Acadamy Program, 1. und 2. Semester“ von Cisco Systems aus dem Markt+Technik Verlag (http://www.mut.de/). Sie können dieses über 1000 Seiten starke Buch auch in unserem Buchshop (http://www.tecchannel.de/abo+shop/buch-shop/) bestellen oder als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Grundlagen zu Routing und Subnetzbildung	434734	S.10
So funktionieren TCP/IP und IPv6	401211	–
Konfiguration und Betrieb eines Nameservers	434393	S. 70

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

1.2 Einführung in VLANs

Ein Virtual LAN unterteilt ein Netzwerk in abgeschirmte Segmente und sorgt so für mehr Sicherheit. Die Teilnehmer eines Segments können sich dabei an beliebigen Orten im physikalischen LAN befinden.

Eine sehr wichtige Technik beim Ethernet-Switching sind VLANs (Virtual LAN, virtuelles LAN). Hierbei werden Workstations und Server mit Hilfe von Switches zu logischen Gruppen zusammengefasst. Alle Geräte in einem VLAN können zunächst nur ausschließlich mit den anderen Geräten im eigenen VLAN kommunizieren, sodass das geswitchte Netzwerk wie eine Anzahl mehrerer, nicht verbundener LANs zu betrachten ist. Es ist häufig schwierig, ein VLAN exakt zu definieren, denn die verschiedenen Hersteller verwenden unterschiedliche Ansätze zur Einrichtung von VLANs.

Unternehmen nutzen VLANs häufig als Möglichkeit, eine bestimmte Gruppe von Benutzern logisch zusammenzufassen. Man kann dies mit einem traditionellen Arbeitsplatz vergleichen, wo mehrere Abteilungen häufig in einem Gebäude unterbracht sind; insofern kann man ein auf die Abteilung begrenztes traditionelles LAN als natürliches Abbild dieser Anforderung betrachten.

Heutzutage sind die Mitarbeiter eines Unternehmens mit ihrem Arbeitsplatz jedoch nicht mehr an einen bestimmten Standort im Unternehmen gebunden, da VLANs die Bildung »logischer« Abteilungsbereiche ermöglicht haben. So werden Mitarbeiter der Marketingabteilung eines Unternehmens zu Mitgliedern des Marketing-VLAN gemacht, während Entwickler und Techniker im Entwicklungs-VLAN platziert werden.

VLANs bieten Sicherheit, Skalierbarkeit und einfacheres Netzmanagement. Router in VLAN-Topologien ermöglichen die Filterung von Broadcasts und bieten Sicherheit und Datenflussmanagement.

1.2.1 Logische Gruppen statt physikalischer Segmente

Ein VLAN ist eine logische Gruppierung von Netzwerkgeräten oder Benutzern, die nicht auf ein physisches Segment beschränkt ist. Die Abbildung 1 zeigt die logische Gruppierung von Workstations in VLANs im Vergleich mit der physischen Gruppierung von Workstations in traditionellen LANs.

VLANs segmentieren geswitchte Netzwerke logisch nach Funktionen innerhalb einer Organisation, nach Projektteams oder nach Anwendungen, nicht jedoch auf einer physischen oder geografischen Basis. So können etwa alle Workstations und Server, die von einer bestimmten Arbeitsgruppe verwendet werden, unabhängig von ihrem Standort im Netzwerk an das gleiche VLAN angeschlossen werden.

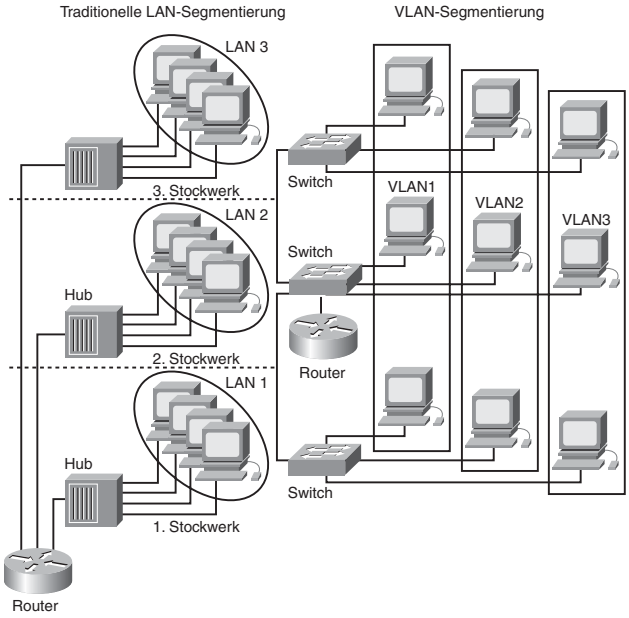


Abbildung 1: LANs und VLANs und ihre physischen Grenzen

Abbildung 2 zeigt ein VLAN-Design, bei dem drei VLANs über zwei Switches hinweg definiert werden, die über einen Router miteinander verbunden sind. Eine Neukonfiguration dieses Netzwerks erfolgt nicht durch physische Trennung und Verlegung von Geräten und Kabeln, sondern einzig über die Konfigura tion der Geräte, d. h. auf einer Softwareebene.

Abbildung 2: VLAN-Design

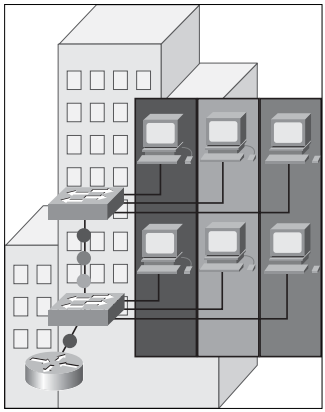


Abbildung 3 zeigt ein VLAN-Design für verschiedene Abteilungen innerhalb des Unternehmens. Hier ist für jede Abteilung – Entwicklung, Marketing und Buchhaltung – jeweils ein VLAN definiert, das sich über drei Switches an drei verschiedenen Standorten erstreckt.

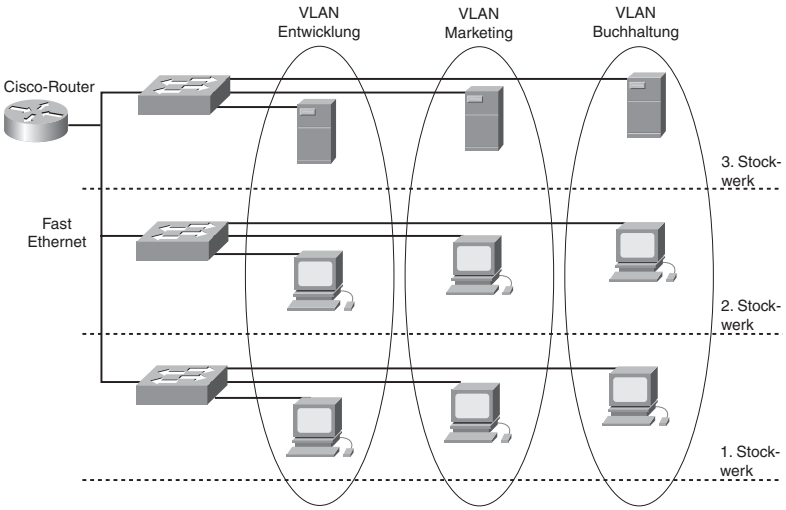


Abbildung 3: VLANs sind nicht auf physische Standorte beschränkt.

Eine Client-Workstation in einem VLAN ist zunächst darauf beschränkt, Dateiserver und Workstations im gleichen VLAN zu kontaktieren. Man kann sich ein VLAN als Broadcast-Domäne vorstellen, die innerhalb einer definierten Gruppe von Switches existiert. VLANs umfassen eine Anzahl von Endsystemen – entweder Hosts oder Netzwerkgeräte wie Bridges und Router –, die durch eine einzige Bridge-Domäne miteinander verbunden sind. Die Bridge-Domäne wird durch verschiedene Netzwerkgeräte wie etwa LAN-Switches realisiert, auf denen Bridging-Protokolle ausgeführt werden; dabei ist für jedes VLAN virtuell eine separate Gruppe von Bridges vorhanden.

1.2.2 Broadcast-Domänen mit VLANs und Routern

VLANs werden erstellt, um die Segmentierung zu ermöglichen, die in traditionellen LANs durch Router realisiert wird. In VLAN-Topologien bieten Router Broadcast-Filterung, Sicherheit und Datenverkehrsmanagement. Switches können den Datenverkehr zwischen VLANs nicht einfach wie eine Bridge weiterleiten, da dies die Integrität der VLAN-Broadcast-Domäne beschädigen würde. Daher muss der Datenverkehr zwischen VLANs immer geroutet werden.

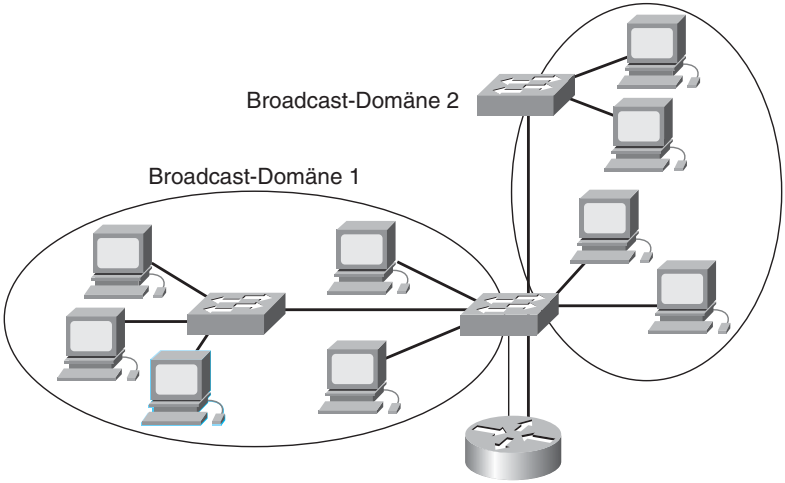


Abbildung 4: Verteilung von Broadcasts im VLAN

Ein VLAN ist eine Broadcast-Domäne, die sich über einen oder mehrere Switches erstreckt. Im folgenden Szenario benötigt das Netzdesign zwei getrennte Broadcast-Domänen. In Abbildung 4 werden mit Hilfe dreier separater Switches zwei getrennte Broadcast-Domänen erstellt. Beachten Sie, dass der Router eine Weiterleitung von Paketen zwischen den Broadcast-Domänen durchführt, die sich wie getrennte Schicht-3-Gruppierungen verhalten. Dazu ist mindestens eine Verbindung zum Router erforderlich.

1.2.3 Betrieb eines VLAN

Ein VLAN bildet ein geswitchtes Netzwerk, das nach Funktionen, Projektteams oder Anwendungen gruppiert wird, ohne dass die physischen Standorte der Benutzer hierbei eine Rolle spielen. Jeder Switch-Port kann einem VLAN zugewiesen werden. Ports, die dem gleichen VLAN zugeordnet sind, verarbeiten auch die gleichen Broadcasts; Ports, die unterschiedlichen VLANs zugewiesen sind, tun dies nicht. Dadurch wird die Gesamtleistung des Netzwerks optimiert, denn die Auswirkung unnötiger, Bandbreite verschwendender Broadcasts wird reduziert.

Man unterscheidet zwei Methoden der VLAN-Konfiguration:

Statische VLANs. Diese Methode heißt auch »portbasierte Mitgliedschaft«. Die Zuordnung eines Ports zu einem VLAN erfolgt durch statische VLAN-Konfiguration. Wenn ein Gerät ans Netzwerk angeschlossen wird, nimmt es automatisch am VLAN »seines« Ports teil. Wechselt der Benutzer die Ports, möchte aber im gleichen VLAN bleiben, dann muss der Administrator eine manuelle Zuweisung des neuen Ports zum gewünschten VLAN vornehmen (Abbildung 5).

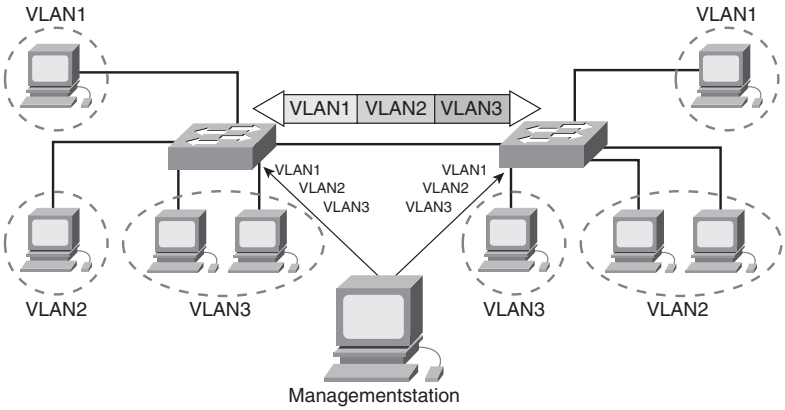


Abbildung 5: Statische VLANs

Dynamische VLANs. Dynamische VLANs entstehen durch den Einsatz von Softwarelösungen wie CiscoWorks 2000. Mit Hilfe eines VMPS (VLAN Management Policy Server, Server für VLAN-Verwaltungsrichtlinien) können Sie Switch-Ports VLANs dynamisch basierend auf der MAC-Adresse des Gerätes zuweisen, das an den Port angeschlossen ist.

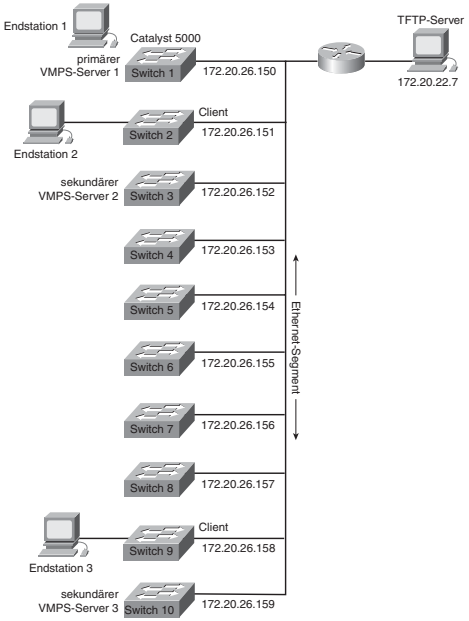


Abbildung 6: Dynamische VLANs

Derzeit ermöglichen die Catalyst-Switches eine Mitgliedschaft in dynamischen VLANs nur basierend auf der MAC-Adresse des Endgerätes. Sobald ein Gerät dem Netzwerk hinzugefügt wird, fragt der Switch den VMPS automatisch zur VLAN-Zugehörigkeit ab (Abbildung 6).

Beispiel: Portzentrisches statisches VLAN

Abbildung 7 zeigt ein statisches, portbasiertes VLAN. Der Port wird einem bestimmten VLAN zugewiesen – abhängig davon, welcher Benutzer oder welches System an ihn angeschlossen ist. Dies bedeutet, dass alle Benutzer, die an den Port angeschlossen werden, Mitglieder desselben VLANs sind. An einen einzelnen Switch-Port sind entweder eine einzelne Benutzer-Workstation oder ein Hub angeschlossen, der wiederum mit mehreren Workstations verbunden ist. Die VLAN-Zuweisung erfolgt in der Regel durch den Netzwerkadministrator. Die Portkonfiguration ist statisch und kann nicht automatisch auf ein anderes VLAN umgeschaltet werden, ohne dass der Switch manuell neu konfiguriert werden müsste. Beachten Sie in der Abbildung 7, dass jedes VLAN sich in einem separaten Subnetz befindet und dass der Router zur Kommunikation zwischen diesen Subnetzen verwendet wird.

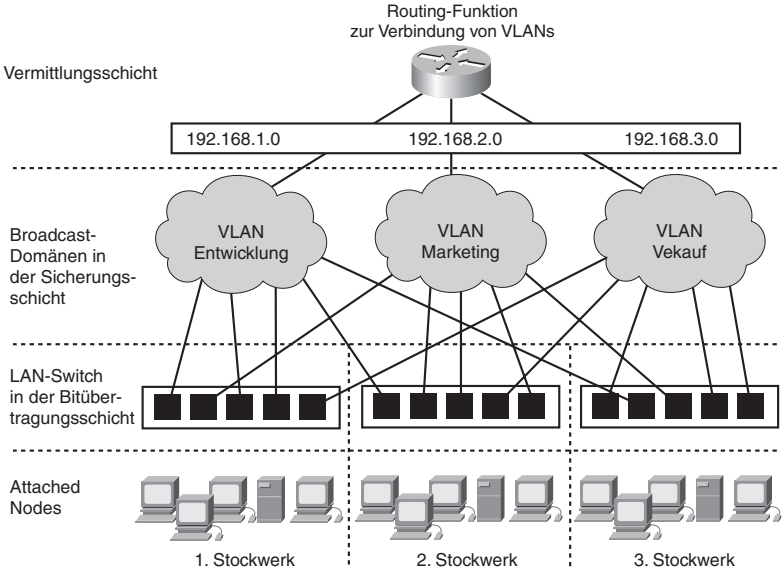


Abbildung 7: Portzentrische statische VLANs

VLANs bieten Benutzern mehr Bandbreite in einem großen Netzwerk, denn sie definieren separate Broadcast-Domänen. Das Standard-VLAN für jeden Port ei-

nes Switchs ist VLAN1, das so genannte Management-VLAN. Es kann nicht gelöscht werden, aber es lassen sich weitere VLANs erzeugen, denen die Ports dann zugewiesen werden können.

Wir erinnern uns: Jede Schnittstelle eines Switchs verhält sich wie ein Port einer Bridge, und Switches sind im Grunde genommen nichts anderes als Multiport-Bridges. Bridges filtern Datenverkehr aus, bei dem Ursprungs- und Zielsegment gleich sind. Muss ein Frame nun eine Bridge passieren und ist die Empfänger-MAC-Adresse bekannt, dann leitet die Bridge den Frame über die korrekte Schnittstelle (und nur über diese) weiter. Weiß die Bridge bzw. der Switch nicht, wo sich der Empfänger befindet, dann flutet er bzw. sie den Frame über alle Ports in der Broadcast-Domäne (VLAN) mit Ausnahme des Herkunftsports.

Ein VLAN muss immer eine eindeutige Schicht-3-Netzwerk- oder Subnetzadresse haben. Dies ermöglicht erst das Schicht-3-Switching von Paketen zwischen VLANs mit Routern. VLANs können entweder als Ende-zu-Ende-Netzwerke, welche die gesamte Switch-Struktur umfassen, oder aber innerhalb geografischer Grenzen existieren.

Ende-zu-Ende-VLANs

Ende-zu-Ende-VLANs (Abbildung 8) ermöglichen eine Gruppierung von Geräten basierend auf den im Netzwerk zu nutzenden Ressourcen. Hierzu gehören Gesichtspunkte wie die Serverauslastung, Projektteams und Abteilungen. Der Zweck von Ende-zu-Ende-VLANs besteht darin, 80 Prozent des Datenverkehrs im lokalen VLAN zu behalten.

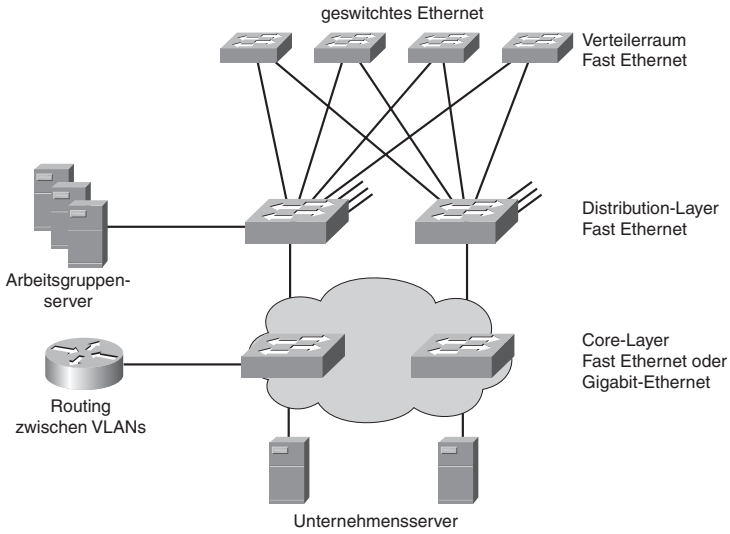


Abbildung 8: Ende-zu-Ende-VLANs

Ende-zu-Ende-VLANs haben die folgenden Eigenschaften:

- Benutzer werden ungeachtet ihres physischen Standorts, aber in Abhängigkeit von ihrer Gruppe oder Arbeitsfunktion zu VLANs zusammengefasst.
- Alle Benutzer in einem VLAN sollten das gleiche Datenflussmuster im Verhältnis 80:20 beim internen und externen Datenaufkommen aufweisen.
- Wenn ein Benutzer innerhalb des Campus umzieht, soll seine VLAN-Zugehörigkeit erhalten bleiben.
- Jedes VLAN hat bestimmte Sicherheitsanforderungen, die für alle Mitglieder gleichermaßen gelten.

Geografische VLANs

Da man in vielen Unternehmensnetzwerken dazu übergegangen ist, die Ressourcen zu zentralisieren, ist die Verwaltung von Ende-zu-Ende-VLANs zunehmend schwieriger geworden. Benutzer müssen viele verschiedene Ressourcen verwenden, von denen wiederum sich längst nicht alle innerhalb ihres VLAN befinden. Angesichts dieser Verschiebung von Ressourcenplatzierung und -verwendung werden VLANs mittlerweile immer häufiger innerhalb enger Grenzen standortbezogen (statt campusweit) erstellt.

Ein solcher geografischer Standort kann ebenso ein vollständiges Gebäude wie auch einen einzigen Switch in einem Verteilerraum umfassen. Innerhalb einer geografischen VLAN-Struktur findet die neue 20:80-Regel normalerweise Anwendung, die besagt, dass 80 Prozent externer Datenverkehr sind, während 20 Prozent lokaler Natur sind – dies ist exakt das Gegenteil der Regel für Ende-zu-Ende-VLANs. Doch auch wenn diese Topologie zur Folge hat, dass 80 Prozent der Ressourcenzugriffe eines Benutzers über einen Router laufen, erlaubt dieses Netzdesign eine logische und folgerichtige Methode des Ressourcenzugriffs.

Geografische VLANs sind außerdem erheblich leichter zu administrieren und zu planen als VLANs, die mehrere geografisch getrennte Bereiche umfassen.

1.2.4 Vorteile von VLANs

Unternehmen strukturieren sich ständig um. Beispielsweise werden in den Vereinigten Staaten jedes Jahr zwischen 20 und 40 Prozent aller Firmenmitarbeiter an andere Standorte versetzt. Diese Verschiebungen, Ergänzungen und Änderungen gehören zu den größten Herausforderungen aller Netzwerkmanager und erhöhen den Aufwand bei der Administration eines Netzwerks beträchtlich. Viele Versetzungen machen eine Neuverkabelung notwendig, und eine Neuadressierung von Stationen wie auch die Umkonfigurierung von Switches und Routern sind in diesem Zusammenhang der Normalfall.

VLANs bieten eine einfache Möglichkeit solcher Änderungen und der Verringerung eines Großteils der Kosten, die mit der Neukonfiguration von Switches und

Routern verbunden sind. Benutzer in einem VLAN nutzen den gleichen Netzwerkadressraum (d. h. das IP-Subnetz) unabhängig von ihrer physischen Position. Wenn Benutzer in einem VLAN von einem Standort an einen anderen verlegt werden, ändern sich ihre Netzwerkadressen nicht, solange sie im ursprünglichen VLAN verbleiben und an einen Switch-Port angeschlossen sind.

Ein Standortwechsel mag lediglich darin bestehen, einen Benutzer an einen Port eines VLAN-fähigen Switchs anzuschließen und diesen Port dann für das entsprechende VLAN zu konfigurieren. Bei dynamischen VLANs konfiguriert der Switch den Port automatisch für das richtige VLAN, sobald die MAC-Adresse der Netzwerkkarte der umgezogenen Workstation beim VMPS abgefragt wurde.

1.2.5 VLANs und Sicherheit

VLANs stellen eine Methode zur Erweiterung der von Routern isolierten Bereiche auf die Switch-Struktur dar und schützen das Netzwerk gegen potenziell gefährliche Broadcasting-Probleme. Ferner sorgen VLANs dafür, dass alle Leistungsvorteile des Switchings beibehalten werden.

Sie erstellen diese geschützten Bereiche, indem Sie Switch-Ports bzw. Benutzern bestimmte VLAN-Gruppen zuweisen. Das ist sowohl innerhalb einzelner Switches als auch über mehrere verbundene Switches hinweg möglich. Broadcast-Datenverkehr innerhalb eines VLAN gelangt nicht aus diesem VLAN heraus. Abbildung 9 zeigt ein Beispiel für Broadcast-Domänen.

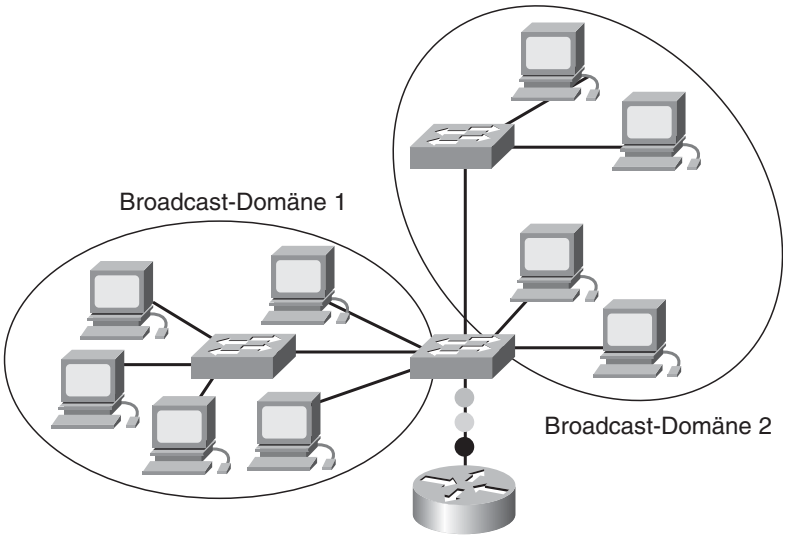


Abbildung 9: Broadcast-Domänen

Umgekehrt erhalten benachbarte Ports den Broadcast-Datenverkehr nicht, der von anderen VLANs erzeugt wird. Diese Form der Konfiguration verringert den Broadcast-Gesamtdatenverkehr erheblich, gibt Bandbreite für echten Benutzerdatenverkehr frei und verringert die Gesamtanfälligkeit des Netzwerks gegenüber Broadcast-Stürmen. Abbildung 10 zeigt, wie ein Router als eine Art Firewall zwischen LANs agieren kann.

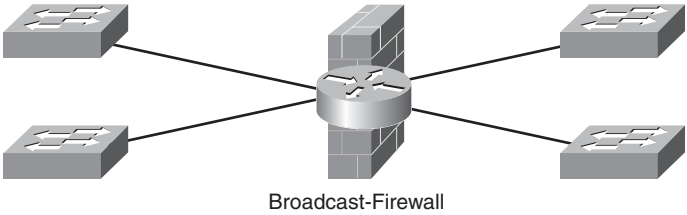


Abbildung 10: Broadcast-Firewall

Ein Problem gemeinsam genutzter LANs besteht darin, dass ein Eindringen in solche Netzwerke vergleichsweise einfach ist. Wenn ein Angreifer eine physische Verbindung mit einem angeschlossenen Port herstellt, kann er auf den gesamten Datenverkehr im Segment sehen. Je größer die Gruppe, desto umfangreicher ist auch der potenzielle Zugriff. Eine kostengünstige und leicht zu administrierende Erhöhung der Sicherheit ist die Segmentierung des Netzwerks in mehrere Broadcast-Gruppen. Dies ermöglicht dem Netzwerkmanager,

- die Anzahl der Benutzer pro VLAN-Gruppe zu beschränken,
- einem Benutzer, dessen Mitgliedschaft zum VLAN noch nicht durch die Managementanwendung (und damit durch den Netzwerkmanager) genehmigt wurde, den Eintritt in eine Gruppe zu verweigern,
- alle nicht benutzten Ports als Low-Service-VLANs zu konfigurieren.

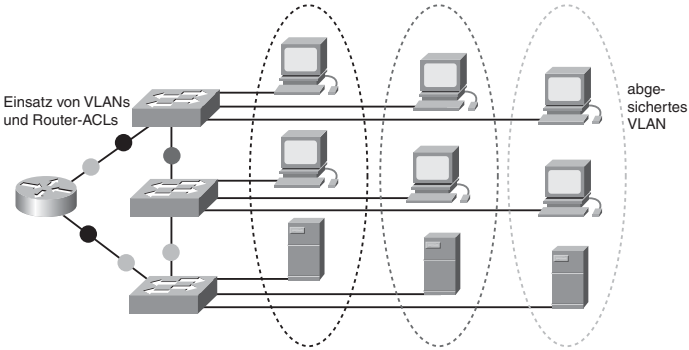


Abbildung 11: Abgesichertes VLAN

Die Umsetzung dieser Form der Segmentierung ist relativ unkompliziert. Switch-Ports werden basierend auf Zugriffsrechten der Anwendungen gruppiert. Eingeschränkte Anwendungen und Ressourcen werden normalerweise in einer gesicherten VLAN-Gruppe abgelegt. In diesem gesicherten VLAN schränkt der Switch oder Router den Zugriff auf die Gruppe ein. Einschränkungen können basierend auf Stationsadressen, Anwendungs- oder Protokolltypen konfiguriert werden. Ein Beispiel für VLAN-Sicherheit zeigt Abbildung 11.

1.2.6 Hubs und nicht VLAN-fähige Switches

Während der letzten Jahre haben Netzwerkadministratoren eine bedeutende Anzahl an Hubs und nicht VLAN-fähigen Switches installiert. Viele dieser Geräte wurden dann durch neuere VLAN-Switches ersetzt. Da jedoch nicht alle Netzwerkanwendungen mehr dedizierte Bandbreite und Leistungsfähigkeit benötigen, können diese Hubs bzw. Switches in vielen Installationen nach wie vor Funktionen erfüllen (Abbildung 12).

Jedes Hub- bzw. Switch-Segment, das mit einem VLAN-Switch-Port verbunden ist, kann nur einem VLAN zugeordnet werden. Alle Stationen innerhalb dieses Segments werden der gleichen VLAN-Gruppe zugewiesen. Der VLAN-Switch arbeitet mit mehreren MAC-Adressen (einer pro Workstation), die dem Port zugewiesen werden, an den der Hub bzw. Switch angeschlossen ist. Wenn später nun eine Station einem anderen VLAN zugeordnet werden soll, dann muss diese an den entsprechenden Hub bzw. Switch angeschlossen werden. Durch den Anschluss von Hubs bzw. Switches an VLAN-Switches können Sie diese älteren bzw. einfachen Geräte als Teil der VLAN-Architektur benutzen.

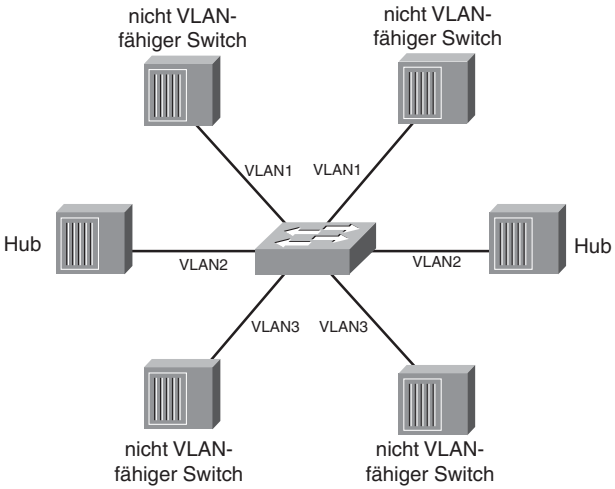


Abbildung 12: Ältere Hubs bzw. Switches in einer VLAN-Umgebung

1.2.7 VLAN-Typen

Es gibt drei Verfahren der Zuweisung ein Paketes zu einem VLAN:

- portbasierte VLANs (statisch)
- auf MAC-Adressen basierende VLANs (dynamisch)
- protokollbasierte VLANs (dynamisch)

Die Anzahl der VLANs im Switch kann aufgrund mehrerer Faktoren variieren. Zu diesen Faktoren gehören Datenverkehrsmuster, Anwendungstypen, Netzmanagementbedürfnisse und Gruppenzugehörigkeit. Ein wesentlicher Aspekt bei der Definition der Switch-Größe und der Anzahl der VLANs ist das verwendete IP-Adressschema. Nehmen wir etwa beispielsweise an, ein Netzwerk verwendet zur Definition der Subnetze eine 28-Bit-Maske. Hieraus ergibt sich, dass insgesamt 14 Hostadressen in einem Subnetz zulässig sind. Da ein 1:1-Verhältnis zwischen VLANs und IP-Subnetzen strikt empfohlen wird, können in jedem VLAN nicht mehr als 14 Geräte vorhanden sein.

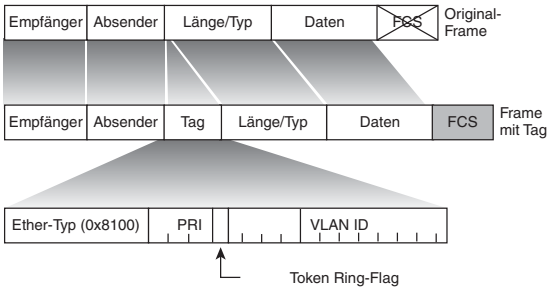
1.2.8 Kennzeichnung von VLAN-Frames

In VLANs mit mehreren Switches werden die Frame-Header gekapselt oder modifiziert, um die Frames mit einer VLAN-Kennung zu markieren, wenn sie über die Leitung zwischen Switches weitergeleitet werden. Vor der Weiterleitung zum Endgerät wird der Header dann wieder in sein Ursprungsformat zurückversetzt. Mit Hilfe dieser VLAN-Kennzeichnung wird logisch ermittelt, welche Pakete zu welcher VLAN-Gruppe gehören. Es gibt mehrere derartige Bündelungsmethoden (engl. Trunking): IEEE 802.1Q, ISL, 802.10 und LANE.

IEEE 802.1Q (Frame-Tagging)

Dieses Protokoll ist eine IEEE-Standardmethode zur Kennzeichnung von VLANs durch Einfügen einer VLAN-Kennung in den Frame-Header. Der Vorgang heißt deswegen auch Frame-Tagging (Frame-Kennzeichnung). Abbildung 13 zeigt das Format eines 802.1Q-Frames.

Abbildung 13: 802.1Q-Frame-Format



Jeder 802.1Q-Port arbeitet als »VLAN-Leitungsbündel« (engl. Trunk) und gehört zum »nativen« VLAN, standardmäßig mit einer VLAN-ID 1. 802.1Q versieht Frames für das native VLAN nicht mit einem Tag. Deswegen könnten normale Stationen an einem 802.1Q-Port die nativen, nicht gekennzeichneten Frames lesen, alle anderen Frames aber nicht (weil diese eben gekennzeichnet sind). Das IEEE 802.1Q-Frame-Tagging ist die bevorzugte Methode für den Austausch von VLAN-Daten zwischen Switches.

ISL

ISL (Inter-Switch Link) ist ein proprietäres Trunking-Protokoll von Cisco, das ebenfalls mehrere Switches miteinander verbindet. Es wird von Switches und Routern gleichermaßen unterstützt. Abbildung 14 zeigt das Frame-Format.

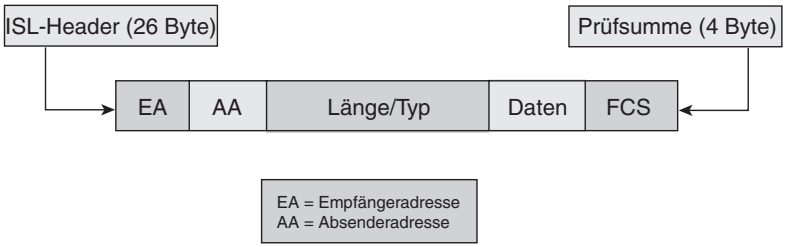


Abbildung 14: ISL-Frame-Format

Die ISL-Kapselung, die von den Switches der Catalyst-Serien verwendet wird, ist eine latenzarme Methode für das Multiplexing von Datenverkehr mehrerer VLANs über einen einzigen physischen Pfad.

Es wurde für Verbindungen zwischen Switches, Routern und Netzwerkkarten implementiert, die in Knoten (z. B. Servern) installiert sind. Um ISL verwenden zu können, benötigte jedes beteiligte Gerät eine ISL-Konfiguration. Ein Router mit mindestens einem ISL-Port wird verwendet, um die Kommunikation zwischen VLANs zu ermöglichen.

Ein Nicht-ISL-Gerät, das ISL-gekapselte Ethernet-Frames empfängt, kann diese als Protokollfehler interpretieren, wenn die Gesamtgröße von Header und Daten-Frame aufgrund der ISL-Kapselung die MTU-Größe (Maximum Transmission Unit) überschreitet.

FDDI 802.10

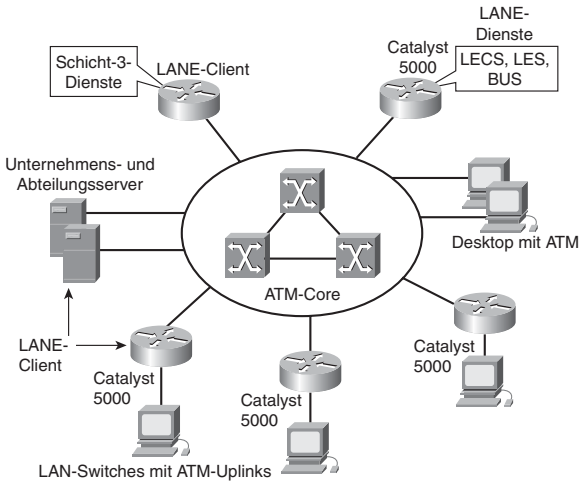
802.10 ist eine proprietäre Methode von Cisco zum Transport von VLAN-Daten innerhalb eines standardkonformen IEEE 802.10-Frames (FDDI, Fiber Distributed Data Interface). Die VLAN-Daten werden in den SAID-Anteil (Security Association Identifier, Sicherheits-ID) des 802.10-Frames geschrieben. Diese Methode wird verwendet, um VLAN-Daten über FDDI-Backbones zu übertragen.

LANE

LANE (LAN Emulation) ist ein durch das ATM-Forum definierter Standard, der zwei Stationen, die über ATM (Asynchronous Transfer Mode) angebunden sind, die gleichen Möglichkeiten wie in herkömmlichen LANs (z. B. Ethernet oder Token Ring) bietet. Wie der Name bereits sagt, besteht die Funktion des LANE-Protokolls in der Emulation eines LAN, die auf ein ATM-Netzwerk aufsetzt. Im Speziellen beschreibt das LANE-Protokoll Methoden zur Emulation von IEEE 802.3-Ethernet- oder 802.5-Token Ring-LANs.

Das LANE-Protokoll definiert eine Dienstschnittstelle für Protokolle übergeordneter Schichten (genauer: der Vermittlungsschicht), die mit der vorhandener LANs identisch ist. Daten, die über das ATM-Netzwerk gesendet werden, werden im passenden LAN-MAC-Format gekapselt, d. h., das LANE-Protokoll sorgt dafür, dass sich ein ATM-Netzwerk so darstellt und auch verhält wie ein Ethernet- oder Token Ring-LAN. Abbildung 15 zeigt ein Beispiel für ein LANE-Netzwerk. Die Tabelle fasst die Methoden für Frame-Tagging und Kapselung zusammen.

Abbildung 15:
LANE-Netzwerk



Frame-Tagging- und Kapselungsmethoden			
Erkennungsmethode	**Kapselung**	**Tagging**	**Medium**
802.1Q	–	✓	Ethernet
ISL	✓	–	Ethernet
802.10	–	–	FDDI
LANE	–	–	ATM

1.2.9 VLAN-Konfiguration

Ursprünglich glaubten die Netzwerkadministratoren, dass VLANs ihre Arbeit erleichtern und Router in Zukunft nicht mehr benötigt würden. Zu ihrem Leidwesen aber war dies eine falsche Annahme: VLANs beseitigen nämlich keine Probleme in Schicht 3. Möglicherweise erleichtern sie den Administratoren die Lösung des einen oder anderen Schicht-3-Problems – z. B. die leichtere Erstellung von ACLs –, aber ohne Schicht-3-Routing geht es nach wie vor nicht.

Statische VLANs konfigurieren

Statische VLANs sind Ports an einem Switch, die einem VLAN durch eine VLAN-Managementanwendung oder durch direkte Konfiguration der Ports statisch zugewiesen sind. Diese Ports behalten ihre VLAN-Konfiguration so lange bei, bis Sie sie selbst ändern. Zwar müssen Änderungen bei statischen VLANs explizit vom Administrator vorgenommen werden, aber dafür sind sie sicher, leicht zu konfigurieren und ohne Aufwand zu überwachen. Statische VLANs sind die richtige Wahl für Netzwerke, für welche die folgenden Bedingungen zutreffen:

- Änderungen müssen verfolgt und administriert werden.
- Es ist eine robuste VLAN-Managementsoftware vorhanden, um die Ports zu konfigurieren.
- Es ist nicht wünschenswert, Zusatzaufwand zur Administration der MAC-Adressen von Endstationen und angepassten Filtertabellen zu betreiben.

Dynamische VLANs hingegen haben keine Ports, die einem bestimmten VLAN zugewiesen sind. Hier basiert die VLAN-Zuweisung vielmehr auf der MAC-Adressierung, der logischen Adressierung oder dem Protokolltyp.

Wichtige Regeln

Beachten Sie die folgenden Grundsätze, wenn Sie statische VLANs an Cisco 29xx-Switches konfigurieren:

- Die maximale Anzahl der VLANs ist Switch-spezifisch und durch die Anzahl der Ports am Switch beschränkt.
- VLAN1 ist das werksseitig für alle Ports vorkonfigurierte VLAN.
- VLAN1 ist das native VLAN.
- CDP- und VTP-Advertisements (Cisco Discovery Protocol, VLAN Trunking Protocol) werden über VLAN1 gesendet.
- An allen Switch-Trunks, die am VLAN teilnehmen, muss das gleiche Trunk-Protokoll (z. B. 802.1Q oder ISL) konfiguriert sein.
- Die Befehle zur Konfiguration von VLANs variieren je nach Switch-Modell.
- Die Management-IP-Adresse eines Catalyst 29xx-Switchs befindet sich standardmäßig in der VLAN1-Broadcast-Domäne.

- Der Switch muss im VTP-Servermodus betrieben werden, damit man VLANs erstellen, hinzufügen oder löschen kann.

Die Erstellung eines statischen VLAN an einem Switch ist eine einfache und unkomplizierte Angelegenheit. Wenn es sich um einen Switch mit nativer IOS-Kommandozeile handelt, wechseln Sie mit Hilfe des Befehls vlan database aus dem privilegierten in den VLAN-Konfigurationsmodus. Die zur Konfiguration notwendigen Schritte sind die folgenden:

```
Switch#vlan database
Switch(vlan)vlan vlan_nummer [vlan_name]
Switch(vlan)exit
```

Bei Bedarf kann auch ein Name für das VLAN konfiguriert werden. Nach Bestätigen des Befehls exit ist das VLAN auf dem Switch vorhanden.

Weitere Konfigurationsschritte

Der nächste Schritt besteht nun darin, das VLAN einer oder mehreren Schnittstellen zuzuweisen:

```
Switch(config)#interface fastethernet 0/3
```

Beim Catalyst 2900-Switch sieht das für VLAN2 so aus:

```
Switch(config-if)#switchport access vlan 2
```

Und beim Catalyst 1900-Switch so:

```
(config-if)#vlan-membership static 2
```

Sie können die Konfiguration mit Hilfe des Befehls show running-configuration wie in folgendem Listing gezeigt überprüfen.

```
Switch#show running-config

Hostname Switch
!
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3

switchport access vlan 2
--- ausgabe weggelassen ---
```

Listing: Ausgabe des Befehls show running-configuration

VLAN-Konfiguration überprüfen

Eine empfehlenswerte Vorgehensweise besteht darin, die Konfiguration des VLAN mit Hilfe der Befehle show vlan (siehe Listing), show vlan brief oder show vlan id kennung zu überprüfen.

```
Switch#show vlan
Virtual LAN ID: 300 (IEEE 802.10 Encapsulation)
vLAN Trunk Interface: FDDI 1/1.10
Protocols Configured: Address: Received: Transmitted:
IP 31.108.1.1 642 645
Virtual LAN ID: 400 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.20
Protocols Configured: Address: Received:Transmitted:
IP 171.69.2.2 123456 654321
Bridge Group 50 5190 8234
Virtual LAN ID:500 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IPX 1000 987654 456789
Virtual LAN ID:600 (ISL Encapsulation)
vLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received:Transmitted:
IP 198.92.3.3 8114 4508
IPX 1001 2 3
Bridge Group 50 8234 5190
```

Listing: Ausgabe des Befehls show vlan

Für alle VLANs treffen die folgenden Aussagen zu:

- Ein erstelltes VLAN bleibt so lange unbenutzt, bis es einem Switch-Port zugewiesen wird.
- Standardmäßig befinden sich alle Ethernet-Ports in VLAN1.
- Geben Sie zwischen den Portnummern keine Leerzeichen ein. Andernfalls gibt der Switch eine Fehlermeldung aus, weil das Leerzeichen zur Abtrennung eines anderen Argumentes vorgesehen ist, das nicht Bestandteil dieses Befehls ist.

VLAN-Konfiguration speichern

Sie können die VLAN-Konfigurationsdatei auf einer Diskette speichern und sie dann auf andere Computer übertragen. Zudem ist es immer nützlich, eine Kopie der VLAN-Konfiguration als Textdatei zu Sicherungs- und Überwachungszwecken aufzuheben. Enthält die Konfigurationsdatei unnötige Zeichen, löschen Sie diese vor dem Speichern. So gehen Sie beim Kopieren der VLAN-Konfiguration vor:

1. Wechseln Sie an der Switch-Konsole in den privilegierten Modus.

2. Wählen Sie im Menü ÜBERTRAGUNG von HyperTerminal den Eintrag TEXT AUF-ZEICHNEN.

3. Wählen Sie, wo die Konfiguration gespeichert werden soll, (z.B. Desktop).

4. Geben Sie als Dateiname VLANconfig.txt ein.

5. Klicken Sie auf STARTEN.

6. Geben Sie am Switch erst den Befehl terminal length 0 und dann den Befehl show run ein.

7. Wenn die Anzeige der Konfigurationsdatei endet, kehren Sie zurück zu HyperTerminal. Wählen Sie erneut TEXT AUFZEICHNEN und dann BEENDEN, um die Datei zu spei-chern und zu schließen.

8. Geben Sie am Switch den Befehl terminal length 24, und löschen Sie ggf. überflüssige Zeichen und Zeilen in der Datei VLANconfig.txt auf dem PC.

VLAN-Konfiguration löschen

Um ein VLAN von einem Switch mit set-Kommandos (CatOS) zu entfernen, geben Sie den Befehl clear vlan vlan_nummer ein (siehe Listing). In diesem Listing wird VLAN 2 durch Eingabe des Befehls clear vlan 2 aus der Domäne entfernt. Es ist wichtig festzuhalten, dass Sie diesen Befehl an einem Switch im VTP-Servermodus absetzen müssen; VLANs können nicht von einen Switch im VTP-Clientmodus gelöscht werden. Im VTP-Transparentmodus können Sie zwar ein VLAN löschen, aber das VLAN wird dann nur am betreffenden Catalyst-Switch gelöscht, nicht jedoch in der gesamten VTP-Domäne. Alle Konfigurations- und Löschvorgänge von VLANs haben an einem transparenten Switch nur lokale Bedeutung.

```
Console>(enable) clear vlan 2
This command will deactivate all ports on vlan2
In the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 2 deleted
```

Listing: Ausgabe des Befehls clear vlan

Das Entfernen eines VLAN von einem Switch unter der nativen Cisco IOS Software verläuft genau so wie das Entfernen eines Befehls von einem Router. Weiter oben haben Sie das VLAN2 an der Schnittstelle FastEthernet0/3 mit Hilfe des folgenden Befehls erstellt:

```
Switch(config-if)#switchport access vlan 2
```

Um dieses VLAN wieder von der Schnittstelle zu entfernen, verwenden Sie die no-Form des Befehls bei aktiver Schnittstelle Fa 0/3:

```
Switch(config-if)#no switchport access vlan 2
```

Wenn Sie ein VLAN löschen, werden alle Ports dieses VLANs inaktiv. Diese Ports bleiben dem gelöschten VLAN zugeordnet und inaktiv, bis sie einem neuen VLAN zugewiesen werden.

1.2.10 Fehlersuche und -behebung bei VLANs

Die Fehlkonfiguration eines VLAN ist einer der häufigsten Fehler in geswitchten Netzwerken. In diesem Abschnitt wollen wir die häufigsten Konfigurationsfehler beschreiben und Lösungen für die Problembehebung in Ihrem geswitchten Netzwerk vorschlagen. Die Tabelle auf der nächsten Seite zeigt VLAN-Probleme der oberen Ebene, die bei einem Router oder Switch auftreten können.

VLAN-Probleme	
Symptome	**Mögliche Ursachen und Abhilfemaßnahmen**
Geringer oder unzuverlässiger Durchsatz des VLAN	• Die angeschlossene Hardware funktioniert nicht einwandfrei. Prüfen Sie die Hardware. • Die Vollduplex- oder Halbduplexeinstellungen sind fehlerhaft. • Es liegt ein Verkabelungsproblem vor. Überprüfen Sie die Anschluss-LEDs, und stellen Sie sicher, dass das Anschlusskabel einwandfrei angeschlossen ist und die maximal zulässige Kabellänge nicht überschreitet.
Die angeschlossene Terminal- oder Modemverbindung kann mit dem Router bzw. Switch nicht kommunizieren.	• Der Terminal- beziehungsweise Konsolenanschluss ist falsch konfiguriert. Stellen Sie sicher, dass Baudrate und Zeichenformat korrekt eingestellt sind. • Prüfen Sie, ob am Router eine Default-Route benötigt wird, um den Switch in einem anderen IP-Subnetz erreichen zu können.
Lokale VLAN-Geräte können nicht mit Remote-Geräten im VLAN kommunizieren, die sich jenseits des Routers befinden.	• Die IP-Adressierung oder Subnetzmaske ist falsch konfiguriert. Prüfen Sie dies mit den cdp-Befehlen bzw. show interface. • Das Default-Gateway ist nicht oder falsch angegeben. Überprüfen Sie Router, Switch, Server und Clients. • Das VLAN ist fehlerhaft konfiguriert. Überprüfen Sie die Portzuweisungen. Beseitigen Sie nicht benötigte Verbindungen zwischen VLANs, wenn ein Port zu mehreren VLANs gehört. • Es liegt ein Konsistenzproblem im VLAN vor. Vergewissern Sie sich, dass die VLANs auf beiden Seiten eines Trunks zueinander passen. • Es liegt ein ISL-Problem vor. Stellen Sie sicher, dass das Trunking korrekt konfiguriert ist, verwenden Sie VLAN 1, und vergewissern Sie sich, dass eine gültige Aktualisierung der VTP-Serverinformationen stattgefunden hat.

Die Angaben zu den Symptomen und zu den möglichen Ursachen und Abhilfemaßnahmen können bei der Ermittlung und Lösung von Problemen sehr hilfreich sein. Wenn Sie vor einem Datendurchsatzproblem stehen, überprüfen Sie, welche Art von Fehler vorliegt. Ursache könnte etwa eine fehlerhafte Netzwerkkarte sein. Kombinationen aus FCS-Fehlern (Frame Check Sequence, Rahmenprüfsequenz), Alignment-Fehlern und Runts weisen in der Regel auf eine fehlende Duplexübereinstimmung hin. Hier ist der Schuldige meist die Autonegotiation (automatische Aushandlung) zwischen den Geräten oder nicht zueinander passende Einstellungen der Geräte an den beiden Enden der Verbindung. Beachten Sie die folgenden Fragen:

- Liegt das Problem auf der lokalen oder der entfernten Seite der Verbindung vor? Bedenken Sie: An einer Verbindung ist immer eine Anzahl von Switch-Ports beteiligt.
- Welchen Pfad nimmt das Paket? Wird es über Trunks oder Nicht-Trunks an andere Switches übertragen?

Wenn Sie feststellen, dass die Anzahl der Kollisionen in der Ausgabe des Befehls show interface rapide zunimmt, kann die Problemursache eine überlastete Leitung sein. Der Legende nach beseitigt geswitchtes Ethernet Kollisionen; die Wahrheit aber ist, dass Switches zwar die Anzahl der Kollisionen minimiert, dass aber im Halbduplexmodus immer noch Kollisionen auftreten können, da zwei Geräte durchaus zur gleichen Zeit einen Kommunikationsversuch starten können.

Beispiel zur Fehlersuche

Ein Beispiel hierfür ist ein Newsserver, auf den gleichzeitig mehrere Clients zuzugreifen versuchen. Der Datenverkehr passiert Router und Switch und landet beim direkt angeschlossenen Server. Gleichzeitig versucht der Server, seinerseits mit den Clients zu kommunizieren.

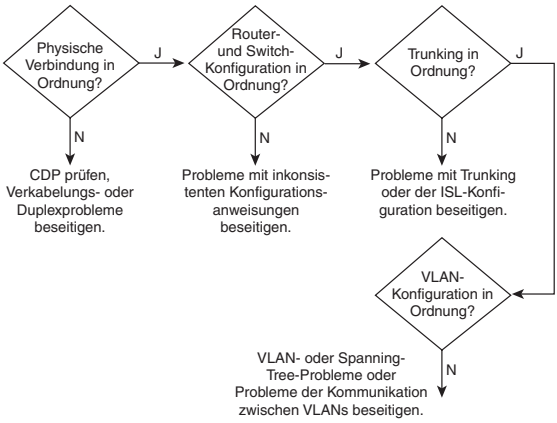


Abbildung 16: Fehlersuche und -beseitigung in VLANs

Während also der Server die Anfrage eines Clients beantwortet, schickt ein anderer Client eine Anfrage – eine Kollision ist also durchaus möglich. Die einzige Möglichkeit, Kollisionen definitiv zu vermeiden, besteht in der Aktivierung des Vollduplexmodus. Abbildung 16 zeigt den Vorgang der Fehlersuche und -beseitigung in VLANs. Wir wollen hier ein Beispiel zur Fehlersuche behandeln. Gehen wir also davon aus, dass ein bestimmtes Gerät nicht mit einem anderen kommunizieren kann. Hier einige Lösungsvorschläge zur Fehlersuche:

- Stellen Sie mit Hilfe des Befehls show interface sicher, dass IP-Adresse, Subnetzmaske und VLAN-Zugehörigkeit der Switch-Ports korrekt sind. Um Konflikte zu vermeiden, müssen Sie gewährleisten, dass die Ports verschiedener VLANs mit IP-Adressen und Subnetzmasken in unterschiedlichen Subnetzen konfiguriert sind.
- Befindet sich der Host im gleichen Subnetz wie der Zielhost, dann vergewissern Sie sich mit Hilfe der Befehle show interface und show port, dass die lokale Switch-Schnittstelle und der Switch-Port, an den der Zielhost angeschlossen ist, dem gleichen VLAN zugewiesen sind.
- Befindet sich der Zielhost in einem anderen Subnetz, dann stellen Sie mit Hilfe des Befehls ipconfig /all an den PCs sicher, dass das Gateway mit der Adresse des jeweiligen Routers im gleichen Subnetz konfiguriert ist.
- Prüfen Sie den Spanning-Tree-Status des Ports mit Hilfe des Befehls show spantree (Catalyst 1900) bzw. show spanning-tree vlan (Catalyst 2950). Befindet sich der Port in den Zuständen Listening oder Learning, dann warten Sie, bis er in den Status Forwarding wechselt, und versuchen Sie dann erneut, eine Verbindung mit dem Host herzustellen.
- Vergewissern Sie sich mit Hilfe des Befehls show port, dass die Geschwindigkeits- und Duplexeinstellungen des Hosts und der entsprechenden Switch-Ports korrekt sind.

Fehlersuche bei Endstationen

Wenn das angeschlossene Gerät eine Endstation ist:

- Aktivieren Sie mit Hilfe des Befehls set spantree portfast enable die portfast-Option am Port (nicht bei Switches der 2900-Reihe). Diese Methode versetzt den Port direkt in den Status Forwarding, d. h., die Modi Listening und Learning werden umgangen .
- Deaktivieren Sie mit dem Befehl set trunk 2/1 off die Möglichkeit, an diesem Port Trunking ohne Ihre Erlaubnis zu nutzen (Sicherheitsrisiko).
- Deaktivieren Sie mit dem Befehl set port channel 2/1-2 off die Kanalbündelung (engl. Etherchannel) mit diesem Port. Sie müssen zu diesem Befehl einen gültigen Portbereich angeben, er kann nicht nur für einen einzigen Port abgesetzt werden.
- Vergewissern Sie sich mit Hilfe des Befehls show cam dynamic, dass der Switch die MAC-Adresse vom Host erlernt.

1.2.11 Zusammenfassung

In diesem Beitrag haben Sie gelernt, dass die VLAN-Implementierung die folgenden Vorteile bietet:

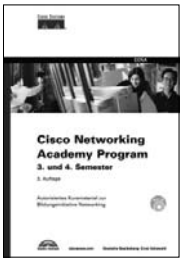
- einfacher Neuanschluss, Umzug und Änderung von Endgeräten
- mehr administrative Kontrolle durch Verwendung eines Schicht-3-Routers zwischen VLANs
- verringerter LAN-Bandbreitenbedarf im Vergleich zu einer einzigen Broadcast-Domäne
- Verringerung der Prozessorbelastung der Endgeräte durch geringere Broadcast-Weiterleitung

Zur Fehlersuche und -behebung bei VLANs haben Sie Folgendes gelesen:

- einen spezifischen Ansatz zur Fehlersuche in VLAN-basierten Netzwerken
- einige der häufigsten Probleme bei der Konfiguration von VLANs und deren Behebung
- Wege zur Vermeidung von Broadcast-Stürmen und Schleifen im Netzwerk
- Befehle zur Fehlersuche und deren Verwendung (ala)

Weiterführende Infos

Dieser Artikel basiert auf dem Kapitel 8 des Standardwerks „Cisco Networking Academy Program, 3. und 4. Semester“ aus dem Verlag Markt+Technik. Sie können dieses über 800 Seiten starke Buch auch in unserem tecCHANNEL-Buchshop unter dem Webcode „buchshop“ bestellen oder als eBook herunterladen.



tecCHANNEL-Links zum Thema	Webcode	Compact
Einführung in VLANs	434093	S.48
VLAN-Performance im Blick	402755	–
Grundlagen zu Routing und Subnetzbildung	434734	S.10

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

2. Dienste und Services

DNS ist ein zentraler Dienst im Internet. Dementsprechend sind die Sicherheit und die richtige Konfiguration eines Nameservers von entscheidender Bedeutung. LDAP bietet einen vollen Verzeichniszugriff über einen TCP/IP-Stack. Das folgende Kapitel widmet sich ausführlich den LDAP-Grundlagen sowie den Aspekten der Sicherheit.

Active Directory ist auf eine Reihe von Diensten und Features angewiesen, um korrekt funktionieren zu können. Wenn einer dieser Dienste ausfällt, ist ein ungewöhnliches oder unkontrollierbares Verhalten die Folge. Dieses Kapitel schildert im zweiten Teil die häufigsten Probleme und liefert die passenden Lösungen.

2.1 Konfiguration und Betrieb eines Nameservers

Der Domain Name Service dient dazu, im gesamten Internet eine aktuelle Datenbasis zu verwalten, die zur Umwandlung von Rechnernamen und IP-Adressen dient. Unsere Praxisserie hilft bei Einrichtung und Betrieb eines Nameservers. In der Anfangszeit des Internets wurde an zentraler Stelle die Datei *hosts.txt* gepflegt, die dann von den Administratoren auf die lokalen Rechner kopiert wurde. Dieses Verfahren ist jedoch nur für kleine Netze praktikabel, so dass ein neuer Service, nämlich der Domain Name Service (DNS), entwickelt wurde. Heute ist die Client-Seite dieses Services Bestandteil aller verbreiteten TCP/IP-Implementationen.

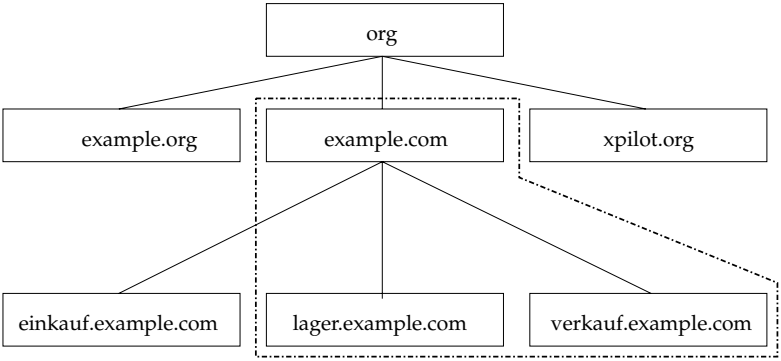
Viele Betriebssysteme werden bereits mit den passenden Server-Programmen geliefert oder diese sind separat erhältlich. Das Internet wäre ohne DNS heute gar nicht denkbar, da die Strukturen viel zu groß, komplex und dynamisch geworden sind. DNS ist heute vermutlich die größte, real existierende und funktionierende verteilte Datenbank.

Auch lokale Netze ab einer gewissen Größe profitieren vom Einsatz eines Nameservers, auch wenn dieses Netz nicht mit dem Internet verbunden ist. Der Verwaltungsaufwand, der durch viele (verschiedene) *hosts*-Dateien entsteht, und Probleme durch inkonsistente Einträge werden vermieden.

Unter Linux und anderen Unix-Systemen kommt als Nameserver das Paket BIND (Berkeley Internet Name Domain) zum Einsatz. Von dieser Implementierung gibt es auch eine Windows-Portierung. Ausführliche Informationen zur Konfiguration und zum stabilen Betrieb eines Nameservers finden Sie in den Quellen zu BIND (www.isc.org/index.pl?/sw/bind/). Das Programm, das die Datenbasis verwaltet und Anfragen der Clients beantwortet, heißt named. Auf der Client-Seite wird die Resolver-Bibliothek verwendet, die mit dem Nameserver kommuniziert.

2.1.1 Das Konzept des Domain Name Service

Die Namensverwaltung im Internet ist hierarchisch aufgebaut. Ganz oben in der Hierarchie stehen die so genannten Root-Nameserver. Diese Rechner sind zunächst für die Auflösung aller Namen zuständig. Bei diesen Rechnern wird eingetragen, dass für einzelne Zonen jeweils ein anderer Nameserver zuständig (authority) ist. Man sagt, dass diese Zone delegiert wurde. Eine Domain, wie man sie aus dem Host-Namen kennt, ist nicht in jedem Fall mit einer DNS-Zone identisch.



Eigene Zonen: Ein Beispiel für verschiedene Zonen. Verschiedene Zonen werden an andere Nameserver delegiert.

Die oberste Zone, die hier nicht näher betrachtet wird, ist .org. Hier wurden die Zonen *example.org*, *example.com* und *xpilot.org* an andere Nameserver delegiert. In unserer Beispiel-Domain betreibt die Abteilung Einkauf einen eigenen Nameserver. Daher ist die Sub-Domain *einkauf.example.com* nicht Bestandteil der Zone example.com. Die Zone ist in der Abbildung durch die gestrichelte Linie markiert.

Eine Zone wird technisch durch einen *NS*-Datensatz im übergeordneten Nameserver bestimmt. Eine Zone kann identisch mit einer Domain sein, es können aber auch für Sub-Domains weitere Nameserver als zuständig definiert sein, die wieder eine eigene Zone verwalten. Diese Trennung ergibt sich oft aus organisatorischen Gegebenheiten, seien es andere Verantwortlichkeiten für die Netzverwaltung oder die räumliche Trennung zwischen einzelnen Abteilungen oder Zweigstellen.

Anwender verwenden in der Regel nur Rechnernamen und keine IP-Adressen, weil gut gewählte Namen leichter zu merken sind. Daher ist der Ausfall des Nameservers oft gleichbedeutend mit dem Ausfall des Netzes. In jeder Zone sollten daher mehrere Nameserver aktiv sein, wobei einer der primäre Nameserver (primary name server) und alle anderen sekundäre Nameserver (secondary name server) sein sollten. Es ist sinnvoll, diese Rechner auf verschiedene Netzsegmente zu verteilen, damit auch beim Ausfall eines Routers oder Hubs immer noch ein Nameserver erreichbar ist. Im Internet sollten der primary und der secondary Name-

server in verschiedenen Netzen liegen und über verschiedene Provider erreichbar sein. Ein Secondary-Server ist praktisch wartungsfrei, da er seine Daten automatisch vom Primary-Server holt. Sie sollten nur gelegentlich einen Blick in die entsprechenden Log-Dateien werfen.

2.1.2 Auswahl eines DNS-Servers

Auch beim DNS-Server haben Sie die Wahl unter verschiedenen Programmen. Das wohl am häufigsten eingesetzte Programm ist BIND, das wir im Folgenden genauer betrachten werden. BIND ist vergleichsweise alt, gut gepflegt und sehr stabil. Besonders für größere Server wird es gerne eingesetzt.

Am anderen Ende der Skala finden Sie *dnrd*. Dies ist ein kleiner und handlicher Nameserver für kleine Netze. Das Besondere an ihm ist, dass er die Datei */etc/hosts* liest und daraus dynamisch die benötigten Zonen generiert. Mit der Option *-s* können Sie Nameserver angeben, die als Forwarder verwendet werden sollen. Damit ist *dnrd* eine interessante Alternative für per Wählverbindung ans Internet angebundene Netze. Ein weiterer Nameserver ist *djbdns*, der von Prof. Bernstein mit Blick auf Sicherheitsaspekte entwickelt wurde. Der Einsatz dieses Programms gilt als Geschmackssache. Wie auch immer, in den folgenden Abschnitten beschäftigen wir uns mit BIND.

2.1.3 Allgemeines zur Konfiguration eines Nameservers

Die Datei */etc/resolv.conf* kann im Vergleich zu einem einfachen DNS-Client unverändert bleiben. In diesem Fall ist der Server auch sein eigener Client, was in den meisten Fällen gewollt sein dürfte (das ist auch der Standardwert, falls keine */etc/resolv.conf* existiert). Es ist aber auch möglich, einen anderen Nameserver zu verwenden, als denjenigen auf dem lokalen Rechner.

Ab der Version 8 des BIND erfolgt die Konfiguration mit Hilfe der Datei */etc/named.conf*. Sollten Sie bereits eine lauffähige Konfiguration einer älteren BIND-Version haben, dann können Sie die Datei */etc/named.boot* mit Hilfe des Skripts *named-bootconf.sh* in das neue Format konvertieren. Anschließend sollten Sie aber die erstellte Datei prüfen und eventuell weitere Anpassungen vornehmen.

Ein Beispiel für einen primären Nameserver finden Sie in Listing unter *Vorteile eines Nameservers*. In dieser Datei werden die Domain und andere globale Daten, wie beispielsweise. das Arbeitsverzeichnis des *named*, festgelegt. Außerdem werden die Namen der zugrunde liegenden Dateien bestimmt. Nach dem Ändern der Datenbasis muss der *named* die Daten neu lesen. Dazu kann man dem Dämon das Signal *SIGHUP* schicken (z. B. mit `kill -HUP $(cat/var/run/named.pid)`) oder das Kommando `rndc reload` verwenden. Mit dem Kommando `rndc restart` kann der Dämon beendet und neu gestartet werden. Ein weiteres wichti-

ges Signal ist *SIGINT*, das den Dämon veranlasst, seine Datenbank in die Datei */var/tmp/named_dump.db* auszugeben. Dies ist für die Fehlersuche manchmal notwendig. Zur Steuerung des Dämons existieren noch diverse weitere Signale, die in der Manpage dokumentiert sind.

2.1.4 Primary Nameserver

Es existieren eine Reihe von Nameserver-Typen. In jeder Zone muss es einen Primary Nameserver geben, der die maßgeblichen (authoritative) Daten für die Zone verwaltet. Aus Gründen der Ausfallsicherheit sollte es in einer Zone mindestens einen weiteren Nameserver geben, der dann als Secondary Server betrieben wird. Die notwendigen Konfigurationen für einen Secondary Server finden Sie im zweiten Teil der Artikelserie. Für Rechner oder Netze, die nur temporär, z. B. mittels PPP, mit dem Internet verbunden sind, kann es sinnvoll sein, einen Caching-Only-Nameserver einzurichten. Der Betrieb eines Nameservers erfordert sowohl zusätzliche Rechenleistung und mehr Speicher auf dem entsprechenden Rechner als auch zunächst einen höheren Administrationsaufwand im Vergleich zum einfachen Editieren der Datei */etc/hosts*. Im Wesentlichen gibt es zwei (zwingende) Gründe dafür, einen eigenen Nameserver zu installieren:

- Sie beantragen eine neue Domain. Besprechen Sie mit Ihrem Provider, wer den Nameserver für diese Domain betreibt. Wollen Sie den Nameserver selbst betreiben, so muss Ihr Provider dies bei sich entsprechend konfigurieren. Oft wird Ihr Provider den Nameserver zunächst für Sie betreiben.
- Sie wollen innerhalb einer bereits bestehenden Domain für einen organisatorischen Bereich einen neuen Nameserver einrichten. Dies müssen Sie mit Ihrem Netzverwalter besprechen, sonst wird Ihr neuer Server nicht als autorisiert anerkannt.

Ein eigener Nameserver hat aber auch Vorteile, egal ob Sie an das Internet angeschlossen sind oder nicht:

- In einem lokalen Netz sind auf jedem Rechner alle anderen Rechnernamen immer bekannt.
- Die Datenbasis ist immer auf allen Rechnern aktuell und konsistent. Die andernfalls auf den verschiedenen Rechnern notwendigen hosts-Dateien veralten schnell und widersprechen sich möglicherweise.
- Die Namensvergabe und IP-Adresszuordnung ist konsistent.
- Wenn Sie den Nameserver selbst betreiben, können Sie die Daten ändern, ohne Ihren Provider einschalten zu müssen.

Im folgenden Listing finden Sie ein Beispiel für die Datei */etc/named.conf* auf einem primären Nameserver. Mit *directory* im Abschnitt *options* wird das Verzeichnis bestimmt, in dem die Dateien dieses Nameservers abgelegt werden.

```
# Konfig-File für den Name-Server options {directory "/etc/
named";};
# Root Name-Server
zone "." {type hint; file "named.root"; };
zone "jochen.org" {type master; file "named.hosts";};
zone "0.0.127.in-addr.arpa" {type master; file "named.lo-
cal";};
zone "168.192.in-addr.arpa" {type master; file "named.rev";};
```

Ein Rechner kann für mehrere Zonen der primäre und/oder sekundäre Nameserver sein. Für jede Zone ist ein Abschnitt *zone* einzufügen und die entsprechenden Daten müssen verfügbar sein.

Jeder Nameserver sollte einen Cache der Anfragen und Antworten anlegen. Dies wird mit dem Schlüsselwort *cache* bewirkt. Beim Start des Nameservers werden alle noch korrekten Daten aus *named.root* erneut in den Cache geladen. Ein Nameserver wird zum Cache-Only-Server, wenn in der Datei *named.boot* keine *primary* oder *secondary* Schlüsselwörter vorhanden sind.

Der Nameserver muss wissen, wo er den maßgeblichen Name-Server für die Root-Domain des Netzwerks findet. Diese Information ist in der Datei *named.root* gespeichert. In vielen Dokumentationen heißt diese Datei auch *root.cache*, was aber deren Verwendung nicht beschreibt. Diese Datei liegt, wie alle anderen Datendateien auch, im Standard Resource Record Format oder auch im Masterfile-Format vor. Eine ausführliche Beschreibung dieses Formats finden Sie im BIND-Operators Guide, eine Einführung in den folgenden Abschnitten.

Der Nameserver im oben angeführten Listing ist primärer (*primary*) Nameserver für die Zone *jochen.org*. Die Datenbasis befindet sich in der Datei *named.hosts* im Verzeichnis */var/named*. Außerdem ist er der primäre Server für die Zonen *0.0.127.in-addr.arpa* und *168.192.in-addr.arpa*, die zum „Reverse-Lookup" dienen. Mehr Informationen zum Reverse-Lookup finden Sie im zweiten Teil der Artikelserie. Im nächsten Schritt müssen die Daten der einzelnen Rechner in die entsprechenden Dateien, deren Namen in der Datei */etc/named.boot* festgelegt wurden, eingetragen werden. Das Format dieser Dateien und die wichtigsten Einträge werden auf den folgenden Seiten genauer erläutert.

2.1.5 Die Datei named.hosts

In der Datei *named.hosts* werden die Daten für alle Rechner in der Zone gespeichert. Das Format und die einzelnen Einträge werden im folgenden Abschnitt beschrieben, da sie auch in den anderen Dateien zur Konfiguration eines Nameservers verwendet werden.

In diese Datei tragen Sie alle Hosts der Zone ein, für die Sie autorisierter Nameserver sind. Wenn Sie auf Ihrem Nameserver viele Zonen eingerichtet haben, werden Sie den Dateinamen sinnvollerweise sprechend wählen, also beispielsweise den Namen der Zone verwenden.

Wenn Sie sehr viele Zonen haben oder Nameserver für mehrere Kunden betreiben, dann kann es sinnvoll sein, die Zonen in verschiedene Verzeichnisse zu sortieren. Im folgenden Listing finden Sie ein Beispiel:

```
   IN     SOA   janus.jochen.org. hostmaster.jochen.org. (
                  1997040101 ;      Serial
                  28800 ;           Refresh 8 hours
                  7200 ;            Retry 2 hours
                  604800 ;          Expire 7 days
                  86400 ) ;         Minimum TTL 1 day
    IN      MX          10 hermes
    IN      NS          janus.jochen.org.
karotte     IN          A           192.168.3.150
mais        IN          A           192.168.3.151
kohlrabi    IN          A           192.168.3.152
bohne       IN          A           192.168.3.154
erbse       IN          A           192.168.3.155
            HINFO       IBM-PC/AT   UNIX-PC
            IN          TXT         "Test mit Text"
```

2.1.6 Das Masterfile-Format

Eine Datendatei für den Nameserver besteht aus einzelnen Sätzen, Resource Records (RR), und wird Masterfile-Format genannt. Ein Datensatz besteht aus den im folgenden Listing dargestellten Teilen.

```
{name}  {ttl}  addr-class  Record Type  Record Specific data
```

Im Feld *name* finden Sie den zum Eintrag gehörenden Namen des Rechners oder der Domain. Das Feld *ttl* enthält die *Time To Live*, die bestimmt, wie lange diese Daten in der Datenbank gespeichert werden. Wird kein Wert angegeben, so ist der Standardwert der im SOA-Satz angegebene. Außerdem kann der Standardwert für die TTL mit dem Schlüsselwort *$TTL* am Anfang der Datei eingestellt werden. Im Internet wird als Adressklasse *IN* verwendet. Das vierte Feld enthält die Satzart, danach folgen die für die Satzart notwendigen Daten. In den Dateien im Masterfile-Format haben eine Reihe von Zeichen eine besondere Bedeutung:

- Der Punkt (.) steht für die aktuelle Domain, für die die Daten gelten sollen.
- Das at-Zeichen (@) steht für das Origin, das ist die Zone, für die der Nameserver zuständig ist.
- Die Zeichen .. im Feld *Name* stehen für die Null-Domain.
- Die Zeichenfolge *\X*, wobei *X* eines der speziellen Zeichen ist, maskiert diese Sonderbedeutung und steht für das Zeichen selbst.
- Die Zeichenfolge *\DDD* mit *D* als Ziffern steht für das Zeichen mit dem ASCII-Code *DDD*.

- Ein Datensatz kann sich über mehrere Zeilen erstrecken, wenn die Daten in runde Klammern () eingeschlossen werden.
- Ein Semikolon (;) leitet einen Kommentar ein, der bis zum Zeilenende geht.
- Der Stern (*) wird im Feld Name bei einigen RR-Typen (z. B. *MX*) speziell interpretiert. Diese spezielle Bedeutung gilt nicht im Datenbereich.

Start Of Authority (SOA)

Ein SOA-Satz (Start Of Authority) markiert den Beginn einer Zone. Der Name (@, das Origin) steht für den Namen der Zone. Hier werden die grundsätzlichen Informationen für eine Zone festgelegt. Das Origin ist der Name des Rechners, der die Daten bereitstellt. Ein Beispiel für einen SOA-Satz finden Sie in dem Listing auf der folgenden Seite. Es gibt höchstens einen SOA-Satz für eine Zone, für die Zone existiert ein NS-Satz in der übergeordneten Zone.

Die verantwortliche Person ist der Betreiber des Nameservers, der bei Problemen und Fragen angesprochen werden sollte. Hier wird seine E-Mail-Adresse angegeben. Dabei wird das at-Zeichen *(@)* durch einen Punkt ersetzt. Oft wird hierfür ein Mail-Aliasname wie *mailto:hostmaster* oder *mailto:dnsadmin* verwendet.

Als weitere Information wird eine Seriennummer verwaltet, die bei jeder Änderung erhöht werden sollte. Sinnvoll ist die Verwendung des Datums und einer Versionsnummer, falls an einem Tag mehrere Änderungen vorgenommen werden. Am 26. Februar 1996 wäre dann eine mögliche Seriennummer *1996022601*. Anhand dieser Seriennummer erkennt ein Secondary-Server, dass neue Daten vorliegen und er einen Zonentransfer durchführen muss. Wenn Sie die Seriennummer versehentlich zu hoch gesetzt haben, dann ist es nicht einfach, dies wieder zu ändern – denn die Secondary-Server würden sich ja nicht mehr synchronisieren.

Der für Refresh angegebene Wert bestimmt die Anzahl Sekunden, nach denen die Slave-Server die Daten erneut prüfen und eventuell transportieren sollen. Retry gibt an, wie lange auf einen Zonentransfer gewartet wird, bevor ein Fehlschlag angenommen wird. Expire bestimmt, wie lange Daten maximal als gültig anerkannt werden. Die Minimum-TTL gibt den Standardwert für die Time-To-Live (TTL) der einzelnen Sätze an.

Lange Time-outs und Expire-Zeiten sorgen für wenig Netzlast beim Update der Daten, aber für längere Wartezeiten, bis Änderungen auf die sekundären Server übertragen wurden. Oft setzt man die Zeiten herab, wenn sich eine größere Änderung ankündigt. Nachdem alle sekundären Nameserver die Daten übernommen haben, kann man zu den alten Werten zurückkehren.

```
name {ttl} addr-class  SOA Origin  Veranwortlicher (
@    IN      SOA    janus.jochen.org. hostmaster.jochen.org. (
                    1997040101 ;      Serial
                    28800 ;           Refresh 8 hours
                    7200 ;            Retry 2 hours
                    604800 ;          Expire 7 days
                    86400 ) ;         Minimum TTL 1 day
```

Beachten Sie, dass der *named* an alle Namen, die nicht mit einem Punkt (.) abgeschlossen sind, das Origin anhängt. Da dies so ist, ist ein vergessener oder überflüssiger Punkt einer der häufigsten Fehler bei der DNS-Konfiguration.

Nameserver (NS)

Für jeden Nameserver in der Zone muss hier ein Eintrag existieren. Mit diesem Eintrag wird eine neue Zone erzeugt und delegiert. Der erste Eintrag ist der Name der Zone, die bearbeitet wird, der letzte Eintrag ist der Name des verantwortlichen Nameservers. Jede Zone sollte mindestens zwei Nameserver (je einen primären und sekundären) besitzen, damit beim Ausfall eines Rechners der Name-Service weiter funktioniert. Diese Rechner sollten außerdem in verschiedenen Subnetzen bzw. im Internet bei verschiedenen Providern angebunden sein. Damit ist auch ein Router- oder Leitungsausfall zu überstehen.

Für jede Zone gibt es zwei, hoffentlich zueinander passende Definitionen für Nameserver: in der übergeordneten Zone, in der die neu definierte Zone delegiert wird, und in der Zone selbst. Nur diese beiden Einträge gemeinsam machen eine vollständig und korrekt delegierte Zone aus.

Eine beliebte Fehlerkonstellation ist, dass ein Nameserver betrieben wird, der nicht autorisiert ist (für den also im übergeordneten Nameserver (Parent-Name-Server) kein NS-Record existiert), oder ein Rechner als (sekundärer) Nameserver eingetragen ist, obwohl dort kein *named* läuft. Wenn ein System im NS-Record eingetragen, aber selbst nicht zuständig ist (also keinen primary- oder secondary-Eintrag in der *named.boot* hat), so spricht man von einer „Lame Delegation“.

```
name {ttl} addr-class NS   Name servers name
           IN         NS   janus.jochen.org.
```

In den Quellen von BIND sind verschiedene Skripten enthalten, die die Zonen nach Fehlern und Inkonsistenzen durchsuchen. Leider sind diese Skripten nur selten bei Linux-Distributionen installiert. Bei kommerziellen Systemen sind sie in der Regel auch nicht vorhanden. Sie sollten in jedem Fall den Quellcode von BIND installieren, die mitgelieferte Dokumentation lesen und sich die Skripten ansehen. Außerdem gibt es externe Pakete wie *dnslint*, die ebenfalls erweiterte Prüfungen durchführen.

Address (A)

Ein A-Satz enthält für jeden Rechner die zugehörige IP-Adresse. Für Rechner mit mehreren IP-Adressen (multihomed Hosts), ist je IP-Adresse ein Satz erforderlich. Weitere Informationen, die in den im Folgenden erläuterten Satzarten gespeichert werden, sind für den Betrieb eines Nameservers nicht erforderlich und werden oft auch nicht gepflegt. Die einzige Ausnahme sind die PTR-Sätze, die für den „Reverse-Lookup“ erforderlich sind.

Für jede IP-Adresse, die in der Zone belegt ist, sollte genau ein A-Record existieren. Für Rechner, die mehrere IP-Adressen haben, sind also mehrere A-Records

aufzunehmen. Dabei kann, wie im folgenden Listing gezeigt, derselbe Name verwendet werden. Es ist in manchen Fällen sinnvoll, einen zusätzlichen Namen einzurichten, der z. B. das betreffende Interface beschreibt.

Die Namen in der ersten Spalte werden hier ohne Domain angegeben. Da der Name auch nicht durch einen Punkt abgeschlossen wurde, wird vom Nameserver automatisch die Zone angehängt. Daher ist der Rechner unter seinem vollen Namen (FQDN) im Nameserver eingetragen. Der Client, d. h. die Resolver-Bibliothek, durchsucht den Nameserver nach einem Namen zunächst mit der angehängten Domain, so dass Benutzer im lokalen Netz diese in der Regel nicht angeben müssen.

```
{name}    {ttl}     addr-class  A    adress
jupiter             IN          A    192.168.30.202
typhon              IN          A    192.168.31.151
                    IN          A    10.0.0.78
```

Für IPv6-Adressen verwenden Sie den Adresstyp A6. In älteren Versionen der IPv6-RFCs wurde der Adresstyp AAAA verwendet, diesen sollten Sie bei neuen Adressen jedoch nicht mehr einsetzen.

Well Known Services (SRV)

Im DNS ist es möglich, weitere Informationen zu Services, die ein Rechner anbietet, zu speichern. In der Regel werden diese Daten nicht gepflegt, so dass man sich auf diese Angaben nicht verlassen kann. Am besten probiert man den entsprechenden Service einfach aus. Wenn die Verbindung hergestellt werden kann, dann bietet der Rechner den entsprechenden Dienst an, andernfalls nicht. In früheren Versionen wurde statt *SRV* der Resource-Typ *WKS* verwendet.

Canonical Name (CNAME)

Ein Rechnername sollte nicht aufgrund der Funktion des Rechners vergeben werden. Dennoch ist es oft sinnvoll, einen Rechner auch unter einem passenden Namen erreichen zu können. Dies findet man z. B. bei ftp-Servern, die auch unter dem Alias-Namen *ftp* erreichbar sind. Weitere Dienste, für die häufig Aliasnamen (oder Nicknames) vergeben werden, sind *www*, *pop3*, *smtp* oder *irc*.

Übernimmt ein anderer Rechner diese Funktion, so muss nicht der Name des Rechners, sondern nur der entsprechende Nickname verändert werden. Damit bleibt den Benutzern verborgen, welcher Rechner tatsächlich den Dienst übernommen hat. Wird kein *CNAME* verwendet, sondern muss der Rechner umbenannt werden, so bedeutet das oft einiges an Konfigurationsaufwand und es ist relativ fehleranfällig.

```
aliases  {ttl}   addr-class  CNAME  Canonical name
jupiter          IN          CNAME  ftp
```

Wird ein Rechner umbenannt, so ist es oft sinnvoll, den alten Namen eine Zeit lang als Nickname zusätzlich zu erlauben. Es sollte jedoch nie ein *MX*-Record (Mail Exchange) auf einen *CNAME* weisen, da ein Mail Transfer Agent dort nicht nachfragen muss (*named* gibt eine entsprechende Warnung aus). In aktuellen BIND-Versionen kann außerdem zu einem *CNAME* keine weitere Information, insbesondere kein *MX*-Record, eingetragen werden.

Domain Name Pointer (PTR)

Ein PTR-Satz (Domain Name Pointer) erlaubt es etwa z. B. anhand einer IP-Adresse, auf den Host-Name zu schließen. Diese Funktion wird in der *in-addr.arpa*-Domain benutzt, also etwa in der *named.rev*-Datei. Damit ist es möglich, auch wenn zunächst nur die IP-Adresse eines Rechners oder Gateways bekannt ist, einen Namen anzuzeigen. Diese Funktion wird z. B. von den Programmen *netstat* oder *traceroute* verwendet. Mehr zum Reverse-Lookup finden Sie Abschnitt Die Datei *named.rev*.

Die PTR-Sätze werden für die Funktion *gethostbyaddr(3)*, die für die Umwandlung der IP-Adressen in Namen zuständig ist, benötigt. Jeder Name im PTR-Satz wird mit einem Punkt abgeschlossen, damit BIND nicht die Domain *in-addr.arpa* anhängt. Sie sollten alle Netzwerkteilnehmer, die eine IP-Adresse haben, in den Nameserver aufnehmen, damit Sie nicht auf einen Nameserver-Time-Out warten, nur weil kein Nameserver-Eintrag für den Reverse-Lookup verfügbar ist.

```
name  {ttl}   addr-class  PTR   real name
155.31        IN          PTR   jupiter.jochen.org
151.31        IN          PTR   typhon.jochen.org
```

Bei IPv6 wird als Domain für den Reverse-Lookup *ip6.arpa* verwendet. Die IPv6-Adressen sind dabei im bekannten Format anzugeben. In älteren Applikationen kommt eventuell noch das „Nibble“-Format zum Einsatz, dann müssen Sie die Domain *ip6.inet* verwenden.

Mail Exchange (MX)

Im Internet wird Mail mit Hilfe des Simple Mail Transfer Protocol (SMTP) übertragen. Dabei wird zwischen dem sendenden und empfangenden Rechner eine TCP/IP-Verbindung aufgebaut.

Ist ein Rechner zum Zeitpunkt des Versendens der Mail nicht erreichbar (oder der Rechner nicht an das Internet, sondern mit UUCP angeschlossen), so kann hier ein anderer, verfügbarer Rechner eingetragen werden, der die Mail annimmt. Ist der Rechner dann wieder erreichbar, so wird die Mail weitergereicht. Niedrigere Werte für die Präferenz entsprechen geringeren „Kosten“.

Diese Funktion wird oft eingesetzt, damit nur auf einem oder zwei Rechnern im Netz Mail angenommen werden muss. Damit konzentriert man die Konfigurationsarbeit und die Verfügbarkeitsprobleme auf wenige Rechner.

Sie sollten sich mit dem Administrator des Rechners abstimmen, wenn Sie einen MX-Satz auf einen fremden Rechner zeigen lassen. Andernfalls wird dieser mit unerwarteter Mail bombardiert und diese geht möglicherweise verloren.

```
name  {ttl}         addr-class  MX preference mail exchange
jupiter.jochen.org  IN          MX 0          hermes
```

Ein weiterer Vorteil eines Mail-Exchangers ist, dass die Mail nicht auf Hunderten oder Tausenden von Rechnern weltweit gesammelt wird und möglicherweise unmittelbar nach dem Neustart des Mail-Servers diesen wieder zum Absturz bringt. Wird aufgelaufene Mail zentral gesammelt, dann liefert nur dieser Rechner massenweise Mail aus und im Problemfall kann man mit dem Administrator dieses Rechners einen langsameren Feed vereinbaren.

Prinzipiell ist es möglich, für alle Rechner einer Domain einen zentralen Mail-Hub vorzusehen. Dazu kann man den Eintrag * als *MX* verwenden. Beachten Sie, dass das nicht unbedingt den Effekt hat, den Sie erwarten: Der *MX* gilt für alle möglichen Namen, nicht nur für diejenigen, die in der *named.data*-Datei eingetragen sind. In den meisten Fällen ist es besser, den betreffenden Einträgen explizit einen *MX*-Eintrag zuzuordnen.

Mail-Exchanger dürfen nicht auf einen *CNAME* verweisen. *named* gibt hier eine entsprechende Warnung aus. Wenn Sie einen zusätzlichen Namen auf Ihrem Mail-Hub annehmen wollen, so müssen Sie bei *sendmail* mit Hilfe des Cw-Eintrags dafür sorgen, dass dieser Name als lokal erkannt wird. Andernfalls gibt sendmail die Fehlermeldung "*local configuration error: mail loops back to myself*" aus.

Text (TXT)

Als zusätzliche Information kann zu jedem Rechner ein beliebiger Text abgelegt werden. Außer, dass dieser Text in Anführungszeichen („) eingeschlossen werden muss, bestehen keine weiteren Einschränkungen. Dieser Typ ist nur selten gepflegt, Netzwerkverwalter bevorzugen es in der Regel, diese Informationen mit Hilfe von SNMP direkt vom betreffenden System auszulesen.

```
name           {ttl}  addr-class  TXT   string
jupiter.jochen.org    IN          TXT   "Ein Text"
Responsible Person (RP)
```

Neben dem Verantwortlichen für den Nameserver kann zu jedem weiteren Eintrag ein Ansprechpartner für diesen Rechner hinterlegt werden. Hier wird wieder das at-Zeichen (@) in der Mail-Adresse durch einen Punkt ersetzt.

Verwalten Sie Ihre Rechner jedoch mit SNMP (Simple Network Management Protocol), so tragen Sie diese Information besser in die Management Information Base (MIB) ein.

```
owner {ttl} addr-class  RP mbox-domain-name TXT-domain-name
jupiter     IN  RP jochen.jochen.org   sysadmins.jochen.org
sysadmins.jochen.org   IN   TXT   "Tel: 4711"
```

2.1.7 Die Datei named.local

Die Datei *named.local* (siehe folgendes Listing), die sich im Verzeichnis */var/named* befindet, enthält die zum eigenen Rechner bzw. zum jeweiligen localhost gehörenden Daten. Die Datei besteht nur aus wenigen Einträgen, die wichtig sind, wenn Benutzer in ihren *~/.rhosts*-Dateien auch den Eintrag *localhost* benutzen wollen und/oder der Rechner *localhost* nicht in der Datei */etc/hosts* enthalten ist.

```
@    IN  SOA   janus.jochen.org. hostmaster.jochen.org. (
                                19860121101 ;      Serial
                                3600  ;           Refresh
                                300  ;            Retry
                                3600000;          Expire
                                14400) ;         Minimum
     IN  NS    janus.jochen.org
0    IN  PTR   loopback.
1    IN  PTR   localost.
```

Die Datei named.rev

Für den normalen DNS-Lookup wird die DNS-Domain verwendet. Mit deren Hilfe wird der zuständige Nameserver ermittelt und dann befragt. Für den Reverse-Lookup wurde eine spezielle Zone generiert, die *in-addr.arpa*. In diesem vom DNS verwalteten Baum sind die IP-Adressen nach den zugehörigen Subnetzen strukturiert. Bei der Delegation der Zonen werden die Bytes der Netzadresse in umgekehrter Reihenfolge verwendet.

In Listing 22.1 sind zwei Zonen eingetragen. Die Zone *0.0.127.in-addr.arpa* wird in der Datei *named.local* verwaltet und repräsentiert das *localnet*, die Rechner mit den Adressen *127.0.0.x*. Die Zone *168.192.in-addr.arpa* steht für die IP-Adressen aus dem reservierten Bereich *192.168.x.y*.

In der Datei *named.rev* wird zu einer IP-Adresse der zugehörige Rechnername vermerkt. Damit ist es relativ schnell und einfach möglich, einen Namen zu einer IP-Adresse zu finden. Diese Funktion nennt man auch Reverse-Lookup. Die Datei *named.rev* liegt im Masterfile-Format vor. Ein Beispiel finden Sie in folgendem Listing. In der ersten Spalte sind die Teile aus der IP-Adresse angegeben, die in der Zonendefinition nicht enthalten sind. Auch hier wird wieder die umgekehrte Reihenfolge verwendet.

Beachten Sie, dass Sie jeden Host-Namen mit einem Punkt abschließen müssen. Andernfalls würde stets die Domain *in-addr.arpa* angehängt. Achten Sie außerdem auf die Konsistenz der Dateien *named.data* und *named.rev*. Dabei kann Ihnen ein Tool wie *dnslint* helfen.

Bei IPv6 wird für den Reverse Lookup die Domain *ip6.arpa* verwendet, als Resource-Record wird weiterhin der Typ PTR verwendet. Noch ist IPv6 nicht weit verbreitet, aber das wird sich ändern.

```
@   IN  SOA  janus.jochen.org. hostmaster.jochen.org. (
                          19860121101 ; Serial
                          10800 ;       Refresh 3 hours
                          3600  ;       Retry   1 hour
                          3600000;      Expire  1000 hours
                          86400 ) ;     Minimum 24 hours
       IN       NS        janus.jochen.org
0.0    IN       PTR       jochen.org
       IN       A         255.255.255.0
151.31 IN       PTR       typhon.jochen.org
155.31 IN       PTR       jupiter.jochen.org
```

Secondary Nameserver

Um die Ausfallsicherheit zu erhöhen, sollten in jeder Zone mindestens zwei Nameserver betrieben werden. Beim Ausfall eines Rechners kann der zweite Nameserver immer noch alle Anfragen beantworten. Damit die Daten stets konsistent sind, darf für jede Zone nur ein (autorisierter) Master-Server existieren.

Daneben können ein oder mehrere sekundäre Nameserver konfiguriert werden. Ein Secondary Nameserver holt seine Daten vom primären Server. Ist dieser nicht verfügbar, so werden die in Sicherheitskopien (*.bak) gespeicherten Daten verwendet. Ist die Time-to-Live der Daten abgelaufen, so wird versucht, diese Daten erneut vom Nameserver zu erhalten. In folgendem Listing finden Sie ein Beispiel für die Datei */etc/named.boot* eines sekundären Nameservers.

```
# conf file excerpt for a secondary name server zone "jochen.
org" {
   type slave;
   masters { 192.168.30.254; };
   file "named.bak";
};

zone "168.192.in-addr.arpa" {
        type slave;
        masters { 192.168.30.254; };
        file "named.rev.bak";
};
```

Anhand der in den SOA-Sätzen der Nameserver-Daten eingetragenen Seriennummern kann ein sekundärer Nameserver feststellen, ob er noch die aktuellen Daten einer Zone besitzt.

Andernfalls kann eine Neuübertragung veranlasst werden. Wenn Sie in den primären Daten eine kleinere Seriennummer vergeben, wird der sekundäre Nameserver entsprechende Meldungen ausgeben. Sie sollten daher die System-Log-Einträge aller Nameserver beobachten, um solche Fehler möglichst auszuschließen. Ansonsten sind Secondary-Server vollkommen wartungsfrei.

2.1.8 Slave-Nameserver

Ein Slave-Server verwaltet keine zonenbezogenen Daten, sondern nur einen Cache und leitet Anfragen, die nicht aus dem Cache beantwortet werden können, an festgelegte Nameserver (forwarders) weiter. Damit kann dieser Rechner einen guten Cache aufbauen, von dem alle Nutzer profitieren können.

Prinzipiell kann jeder Nameserver für die Verwendung von *forward* konfiguriert werden. Dies ist zum Beispiel sinnvoll, wenn der Nameserver nicht direkt an das Internet angeschlossen ist. Wird als Forwarder der Router oder eine Firewall eingetragen, so kann dieser bzw. diese die Anfragen weiterleiten. Ein weiterer Vorteil ist die Ausbildung eines großen Cache, so dass insgesamt weniger Anfragen durch andere Nameserver beantwortet werden müssen.

Forwarder befragen die eingetragenen Server zusätzlich, z. B. zu den bekannten Root-Nameservern. Bei einem Slave-Server werden nur die Forwarder befragt. Können diese keine Antwort liefern, so kann der Host-Name nicht aufgelöst werden. Da diese Rechner die Daten möglicherweise selbst beschaffen müssen, sollten Sie die Adressen mehrfach in der Datei */etc/named.boot* aufführen. Ein Beispiel dafür finden Sie in folgendem Listing.

```
# boot file for slave name server
options {
        directory "/etc/named";
        forward only;
# Unbekannten Anfragen an den DNS der uranus weitergeben
        forwarders {
                194.45.71.65;
                194.45.71.65;
                194.45.71.65;
        };
};
zone "." {
        type hint;
        file "named.root";
};
```

Mit der Option forward-only wird dafür gesorgt, dass nur die angegebenen Forwarder befragt werden. Wenn Sie eine Firewall haben, so kann es sein, dass Sie diese als Forwarder eintragen müssen, wenn die Nameserver keinen Zugang zum Internet haben. Als Vorteil kommt hinzu, dass wiederum die Forwarder einen guten Cache ausbilden können. In alten Versionen von *named* wurde *slave* anstelle der Option *forward only* verwendet.

Sie sollten an erster Stelle den schnellsten (und stabilsten) Nameserver eintragen. Da es möglich (und sogar wahrscheinlich) ist, dass dieser Rechner die Daten zunächst selbst beschaffen muss, sollten Sie den Eintrag für diesen Rechner zwischen die weiteren Forwarder ein- oder zweimal erneut einstreuen.

2.1.9 Weitere Optionen in der Datei named.boot

Das Verhalten von *named* kann durch einige weitere Einträge beeinflusst werden. Die wichtigsten finden Sie hier erläutert, eine vollständige Dokumentation entnehmen Sie bitte dem BIND Administrators Reference Manual, das den BIND-Quellen beiliegt.

`option forward only`

Es werden nur die angegebenen Forwarder befragt. Der früher verwendete Eintrag `slave` sollte nicht mehr verwendet werden. In der Version 8 von BIND hiess die Option `forward-only`.

`logging`

Protokollierung kann sehr flexibel konfiguriert werden. Neben normalen Logs können Sie zur Fehlersuche auch alle Anfragen protokollieren. Logs können mittels `syslog` oder in Dateien geschrieben werden. Wenn Sie besondere Wünsche haben, werfen Sie einen Blick in die BIND-Dokumentation.

`option recursion no`

Normalerweise beschafft ein Nameserver die gewünschten Daten für den Client, selbst wenn er nicht direkt zuständig ist. Das hat den Vorteil der guten Cache-Bildung, würde aber bei den Root-Nameservern, von denen alle Zonen delegiert werden, zu einer sehr grossen Belastung führen. Diese Server liefern nur einen Verweis auf den zuständigen Rechner und nicht die gewünschten Daten. Diesen Eintrag sollten Sie nicht verwenden.

`allow`-Option

BIND9 gestattet es, den Zugriff auf verschiedene Funktionen einzuschränken. Mit der Option `allow-transfer` kann der Zugriff auf die gesamten Zonendaten mittels Zonentransfer auf Rechner aus den angegebenen Netzen beschränkt werden. Damit kann man eine einfache Form der Zugriffskontrolle implementieren. Besonders nützlich ist das nicht, da immer noch die Möglichkeit besteht, die zugeordneten IP-Adressen mittels Reverse-Lookupzu durchsuchen.

Diese Option können Sie auch je Zone angeben, dann wird der Standardwert überschrieben. Weitere Optionen zur Zugriffskontrolle finden Sie in der BIND-Dokumentation erläutert.

`include`

Sie können die Datei `named.boot` aufteilen und die einzelnen Teile mittels `include` einlesen. Das kann interessant sein, wenn Sie viele Zonen verwalten und diese möglicherweise von verschiedenen Personen betreut werden.

`bogus`

Es kann vorkommen, dass fremde Nameserver fehlerhafte Daten liefern. Mit der Option `bogus` lässt sich verhindern, dass ein derartig verseuchter Nameserver befragt wird.

`max-cache-size`

Ein großer Nameserver kann eine beachtliche Last auf eine Maschine bringen. Mit der Option max-cache-size können Sie die Größe des DNS-Cache beschränken. Eine weitere Option, um den Speicherbedarf einzuschränken, ist `recursive-clients`. Hier können Sie die Anzahl der rekursiven Anfragen beschränken, die für Clients durchgeführt werden.

`check-names master|slave|response warn|fail|ignore`

named kann die Namen in den Zonen auf Gültigkeit prüfen. Alte Versionen von BIND ignorierten fehlerhafte Namen stillschweigend, bei aktuellen Versionen kann man wählen, ob *named* eine Warnung ausgeben (warn), einen Fehler melden (fail) oder den Fehler wie gewohnt ignorieren soll (ignore). Die Einstellung kann getrennt für primäre und sekundäre Zonen erfolgen. BIND kennt noch eine ganze Reihe weiterer Optionen. Für viele Fälle werden Sie diese nicht benötigen. Falls Sie etwas vermissen, werfen Sie einen Blick in die BIND-Dokumentation.

2.1.10 Steuerung des named-Prozesses

Das Programm *named*, das den Nameservice bereitstellt, läuft in der Regel als Dämon im Hintergrund. Die Steuerung erfolgt über Signale, die in der Manpage zu *named* dokumentiert sind. Als Vereinfachung existiert das Programm *rndc*, mit dem die wichtigsten Signale versendet werden können. Mögliche Parameter sind:

`stop`

Stoppen des *named*.

`status`

Zeigt die wichtigsten Server-Parameter an, insbesondere die Anzahl der Zonen und ob der Server aktiv ist.

`dumpdb`

named schreibt die aktuelle Datenbank und den Cache in die Datei *named_dump.db*. Diese Funktion ist zur Fehleranalyse manchmal recht nützlich.

`reload [Zone]`

named lädt die angegebene Zone neu. Wenn keine Zone angegeben wird, dann liest *named* die Konfiguration und alle Zonen neu ein.

`stats`

Der Nameserver schreibt seine Statistik in die Datei, die in der Option `statistics-file` angegeben ist. Standardwert ist `named.stats`.

`trace`

Der Tracelevel wird erhöht und mehr Informationen werden in der Datei */var/tmp/named.run* protokolliert.

`notrace`

Der Tracelevel wird um eins verringert und entsprechend weniger Informationen werden protokolliert. `rndc` kann nicht nur auf dem lokalen Rechner verwendet werden. Mit der Option `-s` kann ein anderer Server und mit `-p` ein anderer Port als der Standardwert 953 angegeben werden. Damit das sicher funktioniert, muss der Server mit der Option `controls` konfiguriert werden. Sie können Zugriffe auf IP-Adressen einschränken oder mittels kryptographischen Schlüsseln authentifizieren. In der Standardinstallation kann der Nameserver nur vom localhost aus konfiguriert werden.

2.1.11 Betrieb eines Nameservers

Die Programme aus dem BIND-Paket sind so stabil, dass im täglichen Betrieb kaum mit Problemen zu rechnen ist. Insbesondere ist der Betrieb eines Secondary-DNS praktisch wartungsfrei. Dennoch sollte man ab und zu einen Blick in die Log-Dateien werfen, insbesondere, wenn man die Daten der Zone geändert hat.

Eine solche Änderung ist nicht sofort auf allen Rechnern bekannt. Die Secondary-Server erkennen nach der Erhöhung der `serial`-Nummer, dass sie die Zone neu laden müssen. Das erfolgt normalerweise einmal je `refresh`-Intervall. Treten hierbei Fehler auf, wird der Zonentransfer alle `retry` Sekunden erneut versucht. Die Anfragen werden vom Secondary-Server aber weiterhin als `authoritative` beantwortet, bis die Zeit `expire` abgelaufen ist.

Das heißt, dass es – auch durch das normale DNS-Caching und die Möglichkeit, einen privaten Secondary-Server für fremde Zonen aufzusetzen – keine Möglichkeit gibt, eine Zonenänderung sofort überall wirksam werden zu lassen. Normalerweise wird man tunlichst versuchen, derartige Situationen zu vermeiden, indem man beispielsweise Dienste temporär auf dem alten und dem neuen Rechner parallel anbietet.

Sollte man eine derart plötzliche Umschaltung nicht vermeiden können, so sollte man vorher die Timing-Werte in der Zone schrittweise vermindern (dabei muss auch die `serial`-Nummer erhöht werden). Zum Umschaltzeitpunkt kann man dann mit einer schnellen Verteilung der Daten rechnen. Das bedeutet allerdings, dass in der Zwischenzeit eine deutlich höhere Netzwerklast nur durch DNS-Anfragen zu verzeichnen sein wird.

Ein weiterer Fall, bei dem Sie vorsichtig sein müssen, ist die Verminderung der `serial`-Nummer in einer Zone. Eigentlich ist das nämlich nicht möglich – und Sie sollten es auch zu vermeiden suchen. Wenn Sie es dennoch tun müssen und alle Secondary-Server unter Kontrolle haben, dann können Sie dort die kopierte Zone löschen und die Server neu starten. Im Internet haben Sie normalerweise diesen Zugriff auf die Secondary-Server nicht, so dass Sie hier das in den Quellen zum BIND beschriebene Verfahren (schrittweises und gezieltes Erhöhen der `serial`-Nummer bis zum Überlauf) anwenden müssen.

2.1.12 Dynamische DNS-Updates

Bisher haben wir DNS-Zonen als statisch betrachtet – das stimmt auch, solange nur der Administrator diese ändert. Bei der Verwendung von DHCP ist die Zuordnung von Namen zu IP-Adressen dynamisch möglich. Nun könnte man für alle möglichen IP-Adressen einen statischen Namen vergeben, aber das hat auch Nachteile. Ein Nachteil ist, dass zunächst alle Namen aufgelöst werden können und der Versuch die Rechner dann zu erreichen, in einen Timeout laufen kann.

Mit den Schlüsselwörtern `allow-update` oder `update-policy` im `zone`-Statement kann der Administrator das dynamische Update erlauben. Aus Performance-Gründen wird die Zonen-Datei nicht nach jedem Update neu geschrieben, sondern Änderungen werden zunächst in einem Journal protokolliert. Bei einem Neustart wird dann die bestehende Zone geladen und das Journal nachgefahren. In regelmäßigen Abständen wird allerdings die Zone als Datei gespeichert. Wenn Sie die Zone mit einem Editor ändern wollen, so müssen Sie den Nameserver mit `rndc stop` anhalten und das Journal löschen.

2.1.13 Sicherheit und DNS

DNS ist ein zentraler Dienst im Internet. Bisher hat man sich darauf verlassen, dass schon alles stimmen wird. Programme wie *dnsspoof* beweisen allerdings schon seit geraumer Zeit das Gegenteil. Noch werden die hier vorgestellten Methoden selten eingesetzt, was sich aber hoffentlich ändert. Bisher kann sich ein Client nie sicher sein, ob die Antwort, die er erhalten hat tatsächlich vom authoritativen Nameserver stammt oder nicht. Im Rahmen von DNSsec wurden Methoden entwickelt, dies mit kryptographischen Verfahren sicherzustellen.

Zunächst wird eine Zone wie bekannt erstellt, außerdem wird ein zu dieser Zone gehörendes Keypaar generiert. Die Zone wird mit dem Private Key unterschrieben, so dass Clients anhand des Public Key die Authentität überprüfen können. Ein analoges Verfahren wird bei PGP und GnuPG verwendet. In folgendem Listing finden Sie die notwendigen Befehle, um ein Keypaar zu generieren. Die Keys müssen für das Signieren der Zone verfügbar sein, allerdings kann das auf einem Rechner erledigt werden, der nicht der DNS-Server ist.

```
(linux):~# dnssec-keygen -a rsamd5 -b 2048 -n zone jochen.
org
Kjochen.org.+001+40716
(linux):~# ls -l
...
-rw-r--r--  1 root  jochen   378  29. Apr 21:02
Kjochen.org.+001+40716.key
-rw-------  1 root  jochen  1697  29. Apr 21:02
Kjochen.org.+001+40716.private
...
(linux):~# cat Kjochen.org.+001+40716.key
jochen.org. IN KEY 256 3 1 AQP7qzWpGTD...
(linux):~# dnssec-makekeyset -a Kjochen.org.+001+40716
keyset-jochen.org.
(linux):~# ls -l
...
-rw-------  1 root  jochen   925  29. Apr 21:05 keyset-jo-
chen.org.
```

Der erstellte Public Key wird in die Zone aufgenommen:

```
Zone jochen.org
$INCLUDE Kjochen.org.+001+40716.key
```

Mit dem erstellten Keypaar kann die Zone signiert werden, siehe folgendes Listing. Damit ist das Problem noch nicht gelöst, wie der Public Key zum Client kommt. In abgeschlossenen Umgebungen könnte man diesen manuell transportieren, im Internet wird man eine Public-Key-Infrastruktur aufbauen müssen. In dieser PKI wird der Parent der Zone diese signieren und damit den Key bestätigen.

```
(linux):~# dnssec-signzone -o jochen.org jochen.org
Kjochen.org.+001+40716
jochen.org.signed
```

Beim Signieren der Zone werden zusätzliche NXT- und SIG-Sätze eingefügt, die die Daten authentifizieren. Damit kann ein Client eine Antwort gegen den Public Key prüfen. In dem folgenden Listing finden Sie ein Beispiel für eine Signatur. In der Nameserver- Konfiguration verwenden Sie die Datei *jochen.org.signed* als Zonendefinition.

```
hermes.jochen.org. 86400 IN  MX  10 mail.jochen.org.
                   86400 IN  MX  80 mail.example.org.
                   86400 IN  MX  90 mail2.example.org.
                   86400 SIG     MX 1 3 86400
20020529193717 (
                                 20020429193717 40716
jochen.org.
ksFvd1VtVBjxI+p0RxFWfs4iUCxp0pqhhchr
                                 ...
                                 SvII+aNOpoo51gVy5A== )
```

Der Parent der DNS-Zone signiert das Keyset mit dem Befehl `dnssec-signkey`. Noch ist das unüblich, das könnte sich aber ändern, wenn die DNS-Registrare diesen Dienst anbieten oder sogar zur Pflicht machen.

Zu DNSsec gehört auch noch die Möglichkeit, Anfragen zu signieren (Transaction Signatures, TSIG). BIND9 bietet auch hierfür Unterstützung, primär für Transaktionen zwischen Servern, insbesondere Zonen-Transfers. Das Bind- Handbuch enthält hierfür ein Beispiel, das Sie als Startpunkt verwenden können. Da hier zwischen den Servern ein Shared-Secret verwendet wird, ist es einfach, einen Key zu erzeugen und zu verwenden.

Weitere Informationen zum DNS

Die wichtigsten Informationen zum Betrieb eines Nameservers finden Sie im „Administrators Reference Manual for BIND“, das in den Quellen zu bind enthalten ist.

Empfehlenswert ist ebenso das Buch „Managing DNS and BIND“ von Paul Albitz, Cricket Liu, O‘Reilly and Associates - das Standardwerk zu BIND. (mje)

Weiterführende Infos

Dieser Artikel basiert auf dem Kapitel 22 des Standardwerks „Linux Systemadministration, Einrichtung, Verwaltung, Netzwerkbetrieb“ von Jochen Hein aus dem Verlag Addison-Wesley. Sie können dieses über 600 Seiten starke Buch auch in unserem tecCHANNEL-Buchshop unter dem Webcode „buchshop“ bestellen oder als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Konfiguration und Betrieb eines Nameservers	434832	S.70
So funktionieren TCP/IP und IPv6	401211	–
Ports im Überblick	401852	–
Domain Name System	401207	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

2.2 LDAP

LDAP steht als Abkürzung für Lightweight Directory Access Protocol, die abgespeckte Version des X.500 Directory Service. Hier liegen die Wurzeln von LDAP. In Grunde genommen geht es aber erst einmal um ein Verzeichnis. Ein Verzeichnis ist eine Sammlung von hierarchisch gegliederten Einträgen (Entities). Auch wenn der Begriff LDAP in der Praxis sehr locker verwendet wird, bezeichnet er eigentlich nur ein Protokoll, über das auf die in einem Verzeichnis gespeicherten Daten zugegriffen wird. Die eigentlichen Datenbankfähigkeiten werden von einem separaten Back-End-Programm bereitgestellt.

LDAP definiert also nur ein Protokoll für den Zugriff auf ein solches Verzeichnis. Kurz: ein Nachrichtensatz, der auf bestimmte Datenarten zugreift. Verzeichnisdienste können in verschiedenen Formen auftreten, ihnen sind aber folgende Eigenschaften gemeinsam:

- Ein Verzeichnisdienst ist für Lesezugriffe optimiert. Auf ein Verzeichnis wird fast ausschließlich lesend und selten schreibend zugegriffen. Dies ist ein signifikanter Unterschied zu einer Datenbank.
- Ein Verzeichnisdienst dient nicht nur der Speicherung von Informationen, er implementiert ein verteiltes Modell zur Informationsablage.
- In einem Verzeichnisdienst sind die Informationen in einem Baum organisiert. Es können mehrere Personen für die Administration von Teilbereichen des Baums zuständig sein. Durch die Baumstruktur ist eine effiziente Suche möglich (Suche in Teilbäumen). Verzeichnisdienste besitzen ausgereifte Suchmöglichkeiten. Durch die Baumstruktur in Verzeichnisdiensten lassen sich hierarchische Strukturen wie zum Beispiel Organisationen sehr einfach abbilden.
- Verzeichnisdienste bieten die Replikation zwischen unterschiedlichen Verzeichnisservern zum Datenabgleich an.

Mehrere solcher Verzeichnisdienste existieren bereits: Novells NDS (Novell Directory Services)/Novell eDirectory, Microsoft NTDS (NT Directory Services) bzw. ADS (Active Directory Services), Banyans StreetTalk, OSIs X.500 oder das Domain Name System (DNS).

2.2.1 LDAP-Grundlagen

Das Lightweight Directory Access Protocol ist zwar durch internationale RFCs definiert, jedoch noch kein offizieller Standard. Dennoch kann man bei LDAP von einem De-facto-Standard sprechen. LDAP bietet einen vollen Verzeichniszugriff über einen TCP/IP-Stack und vereinfacht so den Zugriff auf ein X.500-Verzeichnis. Es wurde nur ein Teil der DAP-Funktionen übernommen, allerdings reichen die vorhandenen Funktionen vollständig aus, um den Rest zu emulieren. In der Version LDAPv3 besitzt das Leichtgewicht nur noch neun Kernfunktionen, die allerdings vollkommen ausreichen.

Abfrageoperationen

- search
- read (implementiert durch „search“ mit Mächtigkeit der Ergebnismenge = 1)
- compare

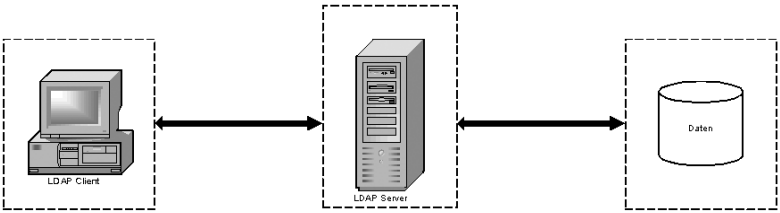
Update-Operationen

- add
- delete
- modifiy
- modifiy DN (rename)

Authentifizierungs- und Kontrolloperationen

- bind (anmelden/authentifizieren)
- unbind (abmelden)
- abandon (Anfrage abbrechen)

Ursprünglich sollte LDAP nur als Mittler zwischen IP-Clients und einem OSI-X.500-Server dienen.



Schema: Zusammenspiel LDAP-Client, LDAP-Server und abzufragende Daten

LDAP ist asynchron, d.h., bei mehreren Anfragen über das Protokoll müssen die Antworten nicht in der gleichen Reihenfolge erfolgen wie die Anfragen. LDAP in seiner Ursprungsversion bildet selbst keinen Verzeichnisdienst – wird aber als „heißer“ Kandidat gehandelt, mit dem eine Integration der unterschiedlichen Verzeichnisdienste gelingt. Alle relevanten Hersteller haben auch bereits eine Unterstützung von LDAP zu ihrem Verzeichnis angekündigt oder bieten sie bereits an. So wie sich IP als Netzprotokoll durchgesetzt hat, wird mit LDAP eine einheitliche Möglichkeit geschaffen, auf Verzeichnisse zuzugreifen.

Der Mehrwert von LDAP beschränkt sich aber nicht nur auf die Interoperabilität zwischen verschiedenen Verzeichnissen und dem Abbild von Benutzerinformationen in einem Unternehmen. Denkbar und bereits in RFC 2307 vorgesehen ist die Speicherung folgender Einträge, um einen Netzwerkinformationsdienst zu bilden:

- Benutzer
- Gruppen
- IP-Dienste (Zuordnung zwischen Namen zu Portnummern und umgekehrt)
- IP-Protokolle
- RPCs (Zuordnung von Remote Procedure Call-Nummern)
- NIS-Netzwerkgruppen
- Boot-Informationen (Boot-Parameter und MAC-Adresszuordnungen)
- Einhängepunkte für Dateisysteme
- IP-Hosts und Netzwerke
- RFC 822-konforme Mailaliase

Aber es ist mehr möglich: Durch Integration von LDAP als „Namensdienstleister" in Anmeldediensten ist auch ein Single Sign-On in heterogenen Umgebungen denkbar. Ein Username/Passwort-Paar regelt den Zugriff auf sämtliche Ressourcen im Netz!

- Anwendung findet der Verzeichnisdienst LDAP z.B. bei:
- Authentifizierung und Speicherung von Benutzern (im Unix-Umfeld Samba, Sendmail)
- Authentifizierung auf Webseiten (Apache, WebDav)
- Namensdienste sowie Ressourcen-Verwaltung (im Unix-Umfeld Hosts usw.)
- Adressbücher kombiniert mit Benutzerverzeichnissen
- Speicherung von Konfiguration von verschiedener Software

LDAP ist als Zugriffsprotokoll auf X.500-Verzeichnisse entworfen worden. Seine Spezifikation beruht auf der Nomenklatur von X.500. Durch Gateways ist es aber nicht mehr auf diesen einen Verzeichnisdienst festgelegt. Die Einträge sind als Objekte verpackt. Sie bestehen aus Attributen mit Typen und Werten und sind in einem hierarchischen Baum strukturiert. Das kennen Sie bereits aus dem hierarchischen Namenssystem von Lotus Domino. Dieser in einer objektorientierten Baumstruktur abgelegte Baum kann über mehrere Server verteilt sein. Jedes Element in diesem Baum ist ein Objekt.

Jedes dieser Objekte hält verschiedene Attribute. Sowohl die Attribute als auch die Objekte unterliegen festen Definitionen: einem LDAP Schema. In diesen Schemata wird definiert, welche Objekte welche Attribute besitzen können. Außerdem ist dort festgelegt, welche Attribute vorhanden sein können und welche vorhanden sein müssen.

Diese Definitionen werden auch Objektklassen (objectClass) genannt. Durch Auswahl dieser Objektklassen in einem Objekt wird diesem zugewiesen, welche Attribute es besitzt. Objektklassen definieren also, welche Attribute mit welchem Wertetyp erlaubt sind. Mögliche Typen sind u.a. IA5 (ASCII)-Zeichenketten, JPEG-Fotos, Sounddaten, URLs und PGP-Schlüssel.

Durch Erweiterung der Schemata lassen sich weitere Strukturen und Definitionen für Attribute hinzufügen. In den Schemata wird außerdem für jeden Objekttyp sowie für die entsprechenden Attribute eine eindeutige Identifikationsmöglichkeit definiert, Unique Object Identifier (OID, Objektkennung) genannt. Diese OIDs werden weltweit eindeutig vergeben.

LDAP-Objekte sind standardisiert, um ein Miteinander einer Vielzahl von Verzeichnisdienst-Servern zu gewährleisten. Ein LDAP-Schema definiert die Liste möglicher Typen von Einträgen (die man als Objektklassen bezeichnet) zusammen mit den mit ihnen verknüpften Attributen. Schema-Definitionen werden in Dateien gespeichert. Bei OpenLDAP liegen die Schema-Dateien im Unterverzeichnis */etc/openldap/schema*.

Die Attribute werden über ihre Datentypen, Formate, Vergleichsmethoden usw. definiert. Innerhalb einer Objektklasse können Attribute erforderlich oder optional sein. Das gleiche Attribut kann Teil von mehr als einer Objektklasse sein.

```
Beispiel für Attributtypen
cn – Common Name
dc – Domain Component
sn – Surname
uid – User ID
```

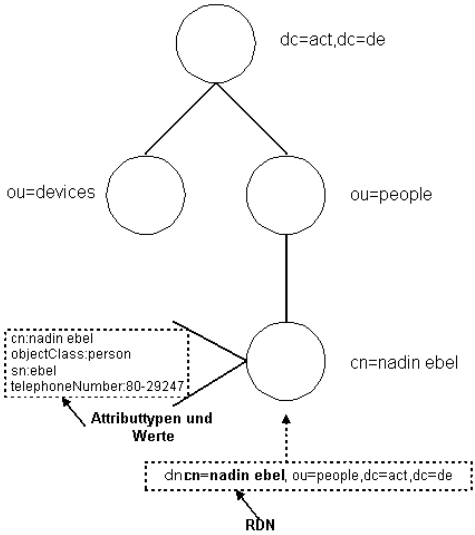
Objektklassen sind hierarchisch angeordnet, wobei die Objektklasse top die Wurzel des Baums bildet. Objekte der ersten Ebene (Level) sind Child-Objekte dieser Klasse und alle darunter liegenden Objektklassen sind deren Nachkommen. Abgeleitete Child-Klassen enthalten automatisch alle Attribute ihrer übergeordneten Parent-Klasse.

```
Beispiel für Objektklassen
person
organization
uidObject
inetOrgPerson
```

Ein Verzeichniseintrag kann in mehreren Objektklassen vorhanden sein.

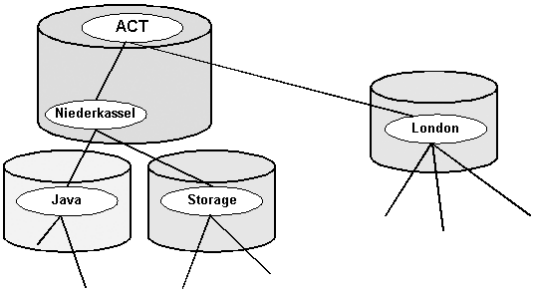
Die hierarchische Baumstruktur wird als Directory Information Tree (DIT) bezeichnet, der den gesamten von einem Server vorgehaltenen Namensraum abbildet (siehe Abbildung). Mit einem oder mehreren Attributtyp-Wert-Paaren, aus denen der so genannte Relative Distinguished Name (RDN) gebildet wird, erhält ein Eintrag einen Namen, der in der Hierarchie-Ebene, in welcher der Eintrag eingeordnet ist, eindeutig sein muss. Durch die Aneinanderreihung der einzelnen RDNs in den verschiedenen Hierarchie-Ebenen von einem Wurzelknoten bis hin zum RDN des Eintrags, wird der so genannte Distinguished Name (DN) gebildet, welcher ein im gesamten Datenbestand eindeutiger Name ist.

Die Unterscheidung in RDN und DN ist wichtig. Wenn der DN wie ein absoluter Pfad zwischen der Wurzel eines Dateisystems und der entsprechenden Datei anmutet, so ist der RDN wie der Dateiname an sich.



Hierarchie: LDAP Directory Information Tree (DIT)

Jedes Objekt hat einen eigenen Eintrag, der die Zugriffsrechte auf das Objekt festgelegt. Diese Zugriffsrechte werden vererbt. Dies ermöglicht eine verteilte Administration, in der unterschiedliche Administratoren für unterschiedliche Teile des Verzeichnisbaumes zuständig sind. Die Daten können auf verschiedene Server, so genannte DSAs (Directory Service Agents) verteilt werden.



Teile und herrsche: Autonomie und verteilte Verwaltungsmöglichkeiten im Tree.

2.2.2 LDAP-Modell

LDAP-Modelle repräsentieren die Dienste, wie sie über den Server bereitgestellt und vom Client gesehen werden. RFC 2251 teilt ein LDAP-Verzeichnis in zwei Komponenten: das Protokoll- und das Datenmodell. In zahlreichen Literaturquellen ist allerdings die Rede von vier Modellen:

Funktionsmodell

Dieses Modell beschreibt die Operationen, die Sie auf den Daten ausführen können wie beispielsweise

- Hinzufügen eines neuen Eintrags
- Löschen eines Eintrags
- Modifizieren eines Eintrags; modifizieren des ausgezeichneten Namens
- Vergleichen eines Eintrags
- Suchen nach Einträgen, die den Suchkriterien genügen

Informationsmodell

Dieses Modell beschreibt, was in einem Verzeichnis abgelegt werden kann. Jeder Eintrag hat einen ausgezeichneten Namen (Distinguished Name, DN) und jeder Eintrag besitzt eine Menge von Attributen, die einen Typ und einen bzw. mehrere Werte haben. Eine besondere Bedeutung haben hierbei die Schemata. Sie beschreiben, in welcher Weise Objekte in Verbindung zueinander stehen (Ober- und Unterklasse) und an welcher Stelle in der DIT-Hierarchie sie auftauchen. Außerdem bestimmen sie, ob Attribute Werte enthalten müssen oder ob sie leer bleiben können. Es ist zwar möglich, dass jeder Server seine eigenen Schemata entwickelt, aber Ziel sollte es sein, dass sich Standards bilden, die zu einer Vereinheitlichung führen.

Namensmodell

Dieses Modell beschreibt, wie Daten angeordnet und angesprochen werden können. Jeder ausgezeichnete Name (DN) besteht aus einer Sequenz von Teilen, so genannte relative ausgezeichnete Namen (Relative Distinguished Name, RDN). Die Einträge eines Verzeichnisses sind in einer hierarchischen Baumstruktur angeordnet (Directory Information Tree, DIT). DIT erlaubt auch Aliase. Aliaseinträge (Verknüpfungen) ermöglichen einen Eintrag an mehreren Stellen im Verzeichnisbaum. Trotzdem muss dieser Eintrag nur an einer Stelle gepflegt werden.

Ein DIT kann auch über mehrere Server verteilt sein. Verweise auf Einträge anderer LDAP-Server erfolgen über LDAP-URLs Da nicht jeder LDAP-Server alle Einträge speichert, ist es nicht nötig, dass der komplette DIT hinterlegt wird. Es ist möglich, dass der DIT auf verschiedene Server aufgeteilt wird. Dadurch werden nur Teilbäume abgebildet, die z.B. die Wurzel nicht abbilden, sondern erst einige Ebenen tiefer aufsetzen. Die oberste Ebene wird als Suffix bezeichnet. Ein Server kann auch verschiedene Bereiche des DIT abbilden, wodurch auf einem Server mehrere Suffixe (Multiple Suffixes) gespeichert werden können.

Um nun aber auf alle Bereiche des DIT zugreifen zu können, müssen die Server Verweise auf andere Server enthalten. Dies wird dadurch realisiert, dass ein Eintrag, an dem der DIT endet, auf ein Suffix eines anderen Servers verweist. Dieser Eintrag wird als Referral bezeichnet.

Sicherheitsmodell

Dieses Modell beschreibt, wie ein Verzeichnis geschützt werden kann. Da innerhalb von Netzwerken große Mengen von sensiblen Daten verschickt werden, ist der Schutz der Daten von wesentlicher Bedeutung. Da insbesondere bei Verzeichnisdiensten viele Personen auf die Daten zugreifen können, muss eine solche Sicherheit gewährleistet werden. Das Problem lässt sich in vier Aspekte unterteilen:

- Authentication (Authentifizierung/Bestätigung) – Es muss sichergestellt sein, dass Sender und Empfänger wirklich die Personen oder Rechner sind, die sie vorgeben zu sein.
- Integrity (Integrität) – Es muss sichergestellt sein, dass die Informationen, die der Empfänger erhält, auch die unveränderten Informationen sind, die der Sender verschickt hat.
- Confidentiality (Vertraulichkeit) – Die Informationen, die versendet werden, dürfen für Außenstehende nicht zu lesen sein (Verschlüsselung der Daten).
- Authorization (Autorisierung) – Es muss sichergestellt sein, dass der Nutzer ausschließlich das machen kann, wozu er berechtigt ist. Dafür ist es notwendig, eine Benutzerkennung einzurichten, die den Nutzer mit Rechten (z.B. lesen, schreiben, löschen) versieht.

Um die Unterschiede zu den normalen relationalen Datenbanken deutlich zu machen, wird eine andere Terminologie verwendet, um die Datenstrukturen eines Verzeichnisdienstes zu benennen: Records (also Datensätze) werden als Einträge (Entries) bezeichnet und jedes Feld innerhalb eines Records wird Attribut genannt.

LDAP definiert den Nachrichtenaustausch, der zwischen dem LDAP-Client und dem LDAP-Server stattfindet. Die Nachrichten, die übermittelt werden, spezifizieren die Operationen, die der Client (Anwender) vornehmen möchte. Außerdem wird die Antwort des Servers übermittelt. Die Nachrichtenübermittlung erfolgt über das TCP/IP-Protokoll, bei dem es sich um ein verbindungsorientiertes Protokoll handelt. Um solche Verbindungen nutzen zu können, muss LDAP über Operationen verfügen, die Sessions (Sitzungen) zwischen Client und Server öffnen und beenden können.

Von besonderem Interesse für ein LDAP-Verzeichnis ist das logische Modell, das hinter dem Verzeichnis steht. Von Bedeutung ist hierbei die Organisation des Verzeichnisses und das Sicherheitskonzept. Im Folgenden wird die grundsätzliche Interaktion zwischen LDAP-Client und Server dargestellt:

1. Der Client öffnet die Session mit einem LDAP-Server, was als „binding" bezeichnet wird. Hierbei werden Host-Name oder IP-Adresse und TCP/IP-Portnummer, über die der LDAP-Server kommuniziert, spezifiziert. Wenn die Verbindung hergestellt ist, muss sich der Client beim Server authentifizieren, wobei unterschiedliche Stärken (z.B. anonym oder per Benutzerpasswort) mit unterschiedlichen Rechten genutzt werden können.

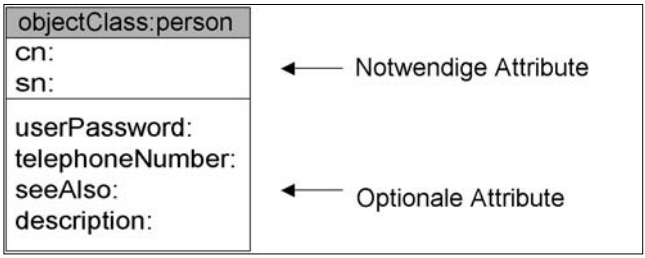
2. Danach gibt der Client die Operationen an, die er vornehmen will. LDAP stellt ihm dabei Lese- und Änderungsoperationen zur Verfügung.

3. Als letzten Punkt muss der Client, nachdem er alle Anfragen erledigt hat, die Session beenden, was als „unbinding“ bezeichnet wird.

Damit Applikationen leichter mit LDAP-Servern kommunizieren können, wurde ein Interface entwickelt. Dieses Interface wird als LDAP API (Application Program Interface) bezeichnet.

2.2.3 Schema

LDAP-Objekte sind standardisiert, um die Zusammenarbeit mit anderen Verzeichnisdienst-Servern zu gewährleisten. Ein LDAP-Schema definiert die Liste möglicher Typen von Einträgen (Objektklassen) zusammen mit den mit ihnen verknüpften Attributen (siehe Abbildung).



Schema: Eine in einem Schema verwendete Objektklasse

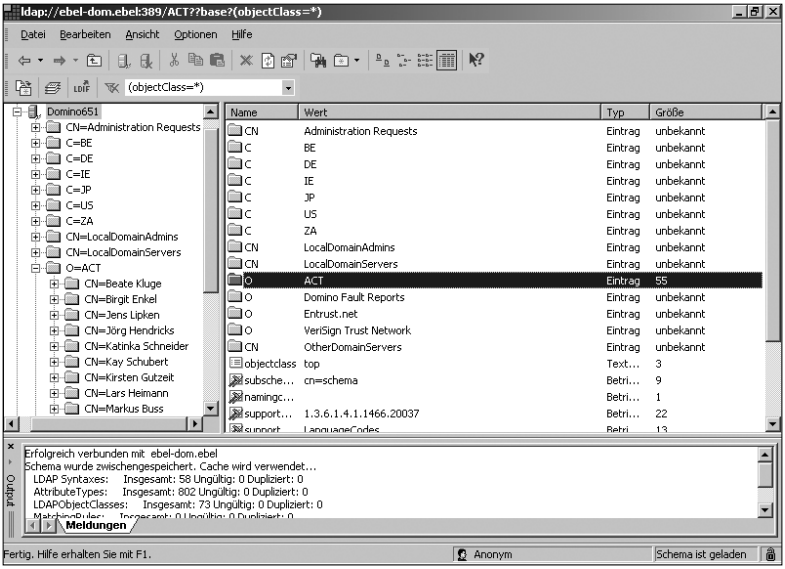
Ein Schema stellt also eine Sammlung von Strukturdefinitionen (Metadaten) dar.

- Definitionen der zu verwendenden Attributklassen
- Definitionen der zu verwendenden Objektklassen
- Filter/Matching-Regeln bei Vergleichsoperationen
- Rechte zum Anlegen und Modifizieren von Datensätzen

Dazu gehören die Beschreibungen der Klassen und der verwendeten Typen. Es gibt verschiedene Schemata und es ist möglich, eigene zu definieren (oder bestehende zu erweitern).

LDAPv3 beinhaltet das Konzept des Schema-Discovery. So ist ein Client in der Lage zu überprüfen, welche Objektklassen, Attribute und Syntaxen der LDAP-Server kennt. Jeder LDAP-Server besitzt ein oder mehrere bekannte Standard-Schemata, auf das man immer zurückgreifen kann. Das heißt, dass jeder, der einen LDAP-Client programmieren will, erwarten kann, dass der LDAP-Server auf bestimmten Standard-Objektklassen und Attributen fußt. Ein Verzeichniseintrag kann in mehreren Objektklassen vorhanden sein. Der LDAP Schema Viewer (ldap.akbkhome.com, www.ldapbrowsers.com) stellt eine praktische Schnittstelle für die Untersuchung von Standard-LDAP-Schema-Objekten zur Verfügung.

Eines der flexibelsten Features von LDAP ist die Tatsache, dass ein Schema erweitert werden kann. Man kann Objektklassen und Attribute ganz nach Bedarf hinzufügen, um die jeweiligen Ansprüche erfüllen zu können.



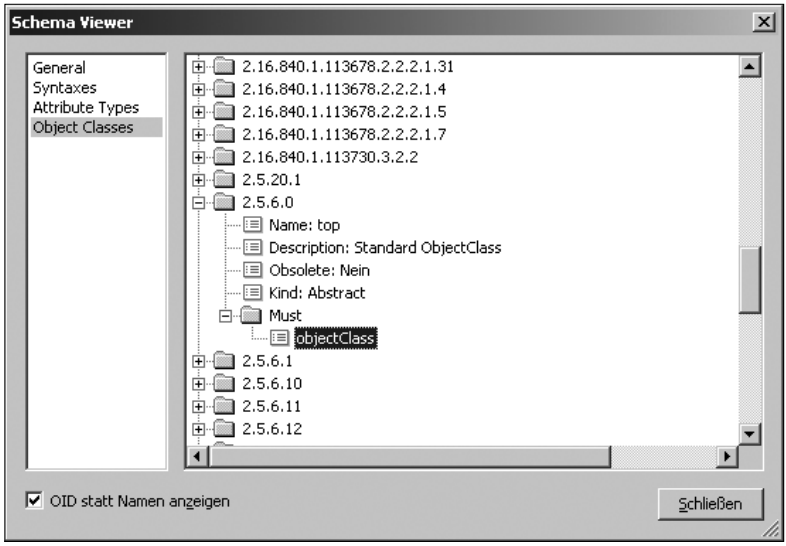
Schema: Verwendung eines LDAP Viewer

Objekt-IDs (OIDs)

Jedes Schema-Element (Attributtypen, Objektklassen, Regeln (Syntax), Matching Rules usw.) besitzt eine weltweit eindeutige Nummer, mit der es identifiziert werden kann – die OID. Dies ist neben einem mehr oder minder sprechenden Namen die zweite Möglichkeit, ein in einem Schema definiertes Objekt zu referenzieren.

Eine Objektkennung (OID) ist eine Zahl, die eine Objektklasse oder ein Attribut in einem Verzeichnisdienst eindeutig kennzeichnet. OIDs werden von Herausgabeinstanzen ausgestellt und bilden eine Hierarchie. Eine OID wird als Zeichenfolge in punktierter Dezimalschreibweise (beispielsweise 1.2.3.4) dargestellt (siehe Abbildung). Organisationen (und Einzelpersonen) können von eine Stamm-OID erhalten und unterhalb dieser weitere OIDs reservieren.

Möchten Sie eigene Objekte für LDAP definieren, benötigen Sie einen Object Identifier (OID). Die Verwendung von OIDs ist also nicht auf einen Verzeichnisdienst beschränkt, sondern bei ASN.1-basierten Protokollen verbreitet. Die Vergabe läuft über die IANA (www.iana.org). Auf der Website des LDAP Schema Viewers haben Sie die Möglichkeit, einige Standard-Schemata zu betrachten.



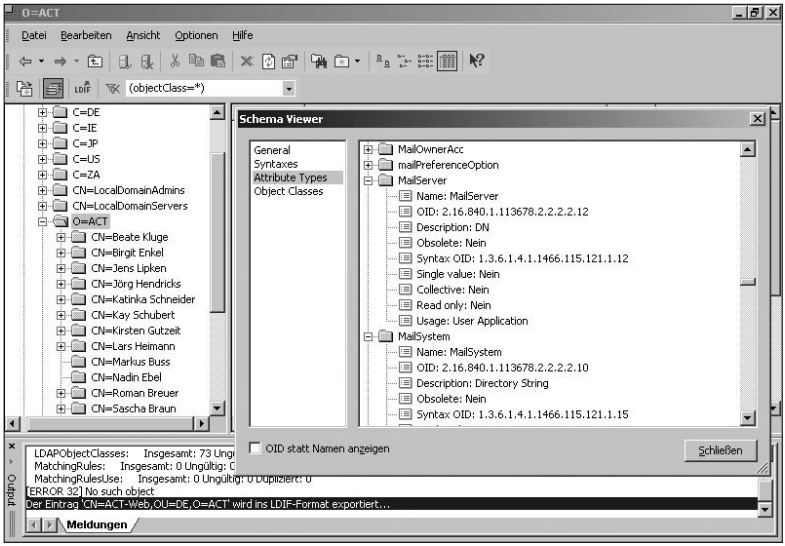
Aufgeteilt: Darstellung von Objektklassen nach OIDs

Attributtypen

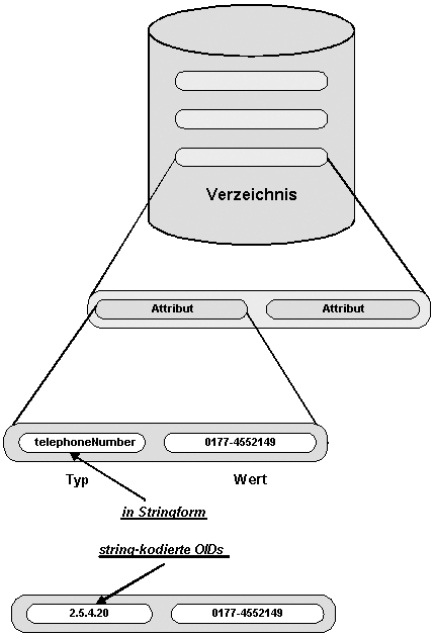
In einem Schema werden Attribute unabhängig von den Objektklassen definiert. So ist es möglich, Attributklassen nicht nur in einer Objektklasse zu verwenden. Das Attribut TELEPHONENUMBER wird in zahlreichen Objektklassen verwendet und sieht als Definition im OpenLDAP core.schema folgendermaßen aus:

```
# attributetype definition telephoneNumber
# basierend auf RFC 2256
attributetype
(2.5.4.20 NAME 'telephoneNumber'
DESC "Telefonnummer"
EQUALITY telephoneNumberMatch
SUBSTR telephoneNumerSubstringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32})
```

Die Definition eines Attributtypen beinhaltet u.a. Namen (telephoneNumber), OID (2.5.4.20), Beschreibung (DESC), Angabe, ob Mehrfachwerte für dieses Attribut zugelassen sind (SINGLE-VALUE, in diesem Beispiel nicht gegeben), Attributsyntax (SYNTAX), Matching Rules (Treffer-Regeln) für die Gleichheit (EQUALITY) und die Gleichheit von Teilzeichenketten (SUBSTR) sowie Längenbeschränkung (Angabe in geschweiften Klammern hinter der Syntaxangabe).



Detailansicht: Attributtypen im LDAP Viewer



Struktur: Einträge und Attribute

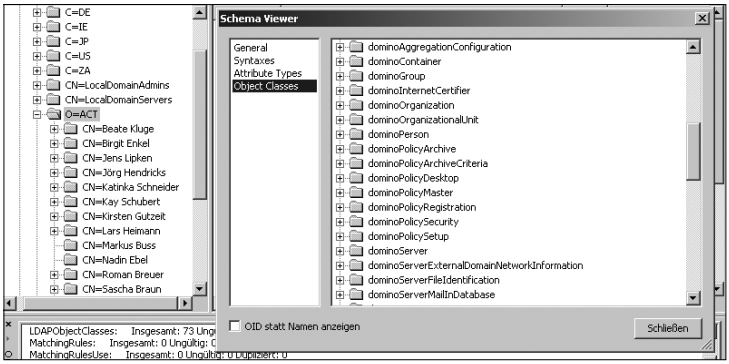
RFC 2252 realisiert die Definition von Attributtypen mithilfe der Backus-Naur-Form-(BNF-)Grammatik, die als eine Beschreibungssprache für Syntaxregeln fungiert. Dies sieht dann (ein wenig kryptisch) so aus:

```
AttributeTypeDescription = „(„ whsp
numericoid whsp                  ; AttributeType identifier
 [ "NAME" qdescrs ]              ; name used in AttributeType
 [ "DESC" qdstring ]             ; description
 [ "OBSOLETE" whsp ]
 [ "SUP" woid ]       ; derived from this other AttributeType
 [ "EQUALITY" woid               ; Matching Rule name
 [ "ORDERING" woid               ; Matching Rule name
 [ "SUBSTR" woid ]               ; Matching Rule name
 [ "SYNTAX" whsp noidlen whsp ] ; see section 4.3
 [ "SINGLE-VALUE" whsp ]         ; default multi-valued
 [ "COLLECTIVE" whsp ]           ; default not collective
 [ "NO-USER-MODIFICATION" whsp ]; default user modifiable
 [ USAGE" whsp AttributeUsage ] ; default userApplications
➥ whsp ")"
AttributeUsage =
"userApplications"     /
"directoryOperation"   /
"distributedOperation" / ; DSA-shared
"dSAOperation"        ; DSA-specific, value depends on server
```

Dabei ist `whsp` ein Leerzeichen (`' '`), `numericoid` eine globale eindeutige OID in numerischer Form (z.B. 1.2.3), `qdescrs` ein oder mehrere Namen, `woid` entweder ein Name oder OID und `noidlen` ein optionales Längenspezifikationssymbol (beispielsweise {10}).

Objektklassen

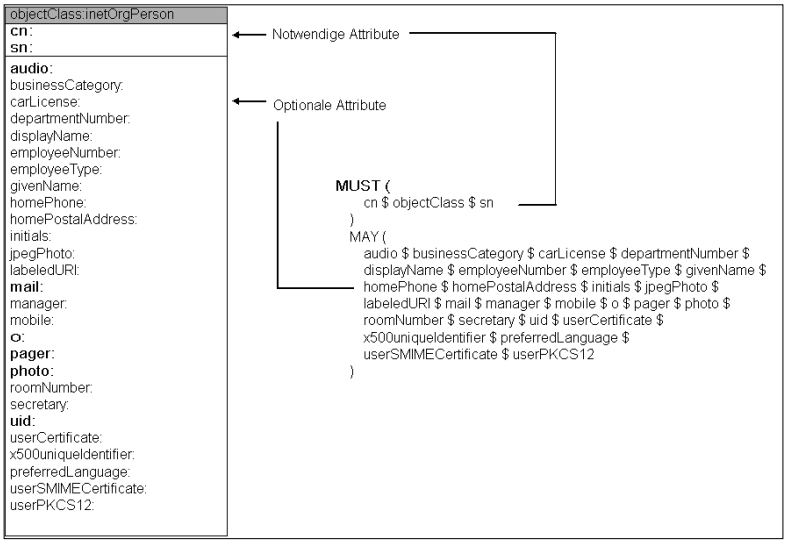
Die `objectclasses`-Direktive dient dem Definieren einer neuen Objektklasse.



Klassenübersicht: Objektklassen im LDAP Viewer

Diese Direktive verwendet die gleiche Objektklassenbeschreibung (wie in RFC 2252 beschrieben) wie im `objectClasses`-Attribut, welche im `subschema subentry` gefunden wird, z.B.:

```
objectclass <RFC2252 Object Class Description>
```



Im Beispiel: Die Objektklasse inetOrgPerson

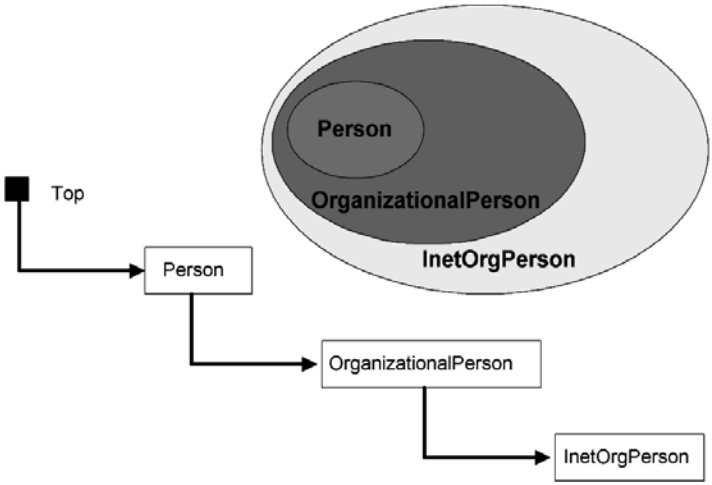
Dabei wird die Objektklassenbeschreibung von dem folgenden BNF definiert:

```
ObjectClassDescription = "(" whsp
     numericoid whsp      ; ObjectClass identifier
     [ "NAME" qdescrs ]
     [ "DESC" qdstring ]
     [ "OBSOLETE" whsp ]
     [ "SUP" oids ]       ; Superior ObjectClasses
     [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
               ; default structural
     [ "MUST" oids ]      ; AttributeTypes
     [ "MAY" oids ]       ; AttributeTypes
        whsp ")"

Objectclass (2.16.840.1.113730.3.2.2
NAME 'inetOrgPerson'
DESC 'RFC 2798: Internet Organizational Person'
SUP organizationalPerson
STRUCTURAL
```

```
MAY(
  audio $ businessCategory $ carLicense $ departmentNumber $
  displayName $ employeeNumber $ employeeType $ givenName $
  homePhone $ homePostalAddress $ initials $ jpegPhoto $
  labeledURI $ mail $ manager $ mobile $ o $ pager $ photo $
  roomNumber $ secretary $ uid $ userCertificate $
  x500uniqueIdentifier $ preferredLanguage $
  userSMIMECertificate $ userPKCS12)
)
```

Die meisten Elemente dieser Objektklassendefinition kennen Sie bereits von der Attributklassendefinition. Die Elemente einer solchen Objektklasse bestehen aus Name, OID, Liste von Attributtypen (`MUST`), Liste von optionalen Attributen (`MAY`), Art der Objektklasse (hier: `structural`), Verweis auf die „Superklasse“ (hier: `organizationalPerson`). Von dieser Klasse werden Attribute übernommen (siehe Abbildung).



Vererbung: Ableitung von Klassen

Objektklassen lassen sich in folgende Typen unterteilen:

1. Eine Objektklasse sollte als `structural` deklariert werden, wenn sie elementare Attribute eines Objektes definiert. Beim Beispiel der Objektklassen zur Beschreibung von Personen ist dies die Objektklasse Person und damit ihre Subklassen. X.501 fordert, dass ein Eintrag immer von mindestens einer als structural deklarierten Klasse abgeleitet ist. Andererseits legt X.501 auch fest, dass nur eine Klasse eines Eintrags überhaupt strukturelle Klassen in ihrem Ableitungsbaum enthalten darf. ITU X.501 stellt eine Reihe von Modellen für das Verzeichnis als Rahmenstruktur für andere Empfehlungen der X.500-Serie vor.

2. Eine als `auxiliary` definierte Objektklasse fügt neue Eigenschaften zu einem Eintrag hinzu, determiniert aber nicht den Typ des Eintrages, der durch seine strukturelle Klasse bestimmt wird. Es ist gewissermaßen der Regelfall, dass eine Objektklasse vom Typ auxiliary ist. Es ist eigentlich nur dann gerechtfertigt, eine eigene Klasse als structural zu definieren, wenn darauf eine völlig neue Objekthierarchie aufgebaut wird.

3. Einige wenige Objektklassen sind weder als structural noch als auxiliary, sondern als `abstract` deklariert. Dieses Konzept entspricht den abstrakten Klassen, wie sie aus der objektorientierten Programmierung bekannt sind: Abstrakte Klassen sollen nicht initialisiert werden, sondern dienen als Vorlage, um von ihnen abgeleiteten konkreten Klassen bestimmte Eigenschaften zu geben. Beispiele für abstrakte Klassen sind die Objektklassen `top` und `alias`, die zur Beschreibung der Struktur des Verzeichnisbaumes verwendet werden.

Aggregation und Federation/Referral: Aggregation beschreibt das Sammeln von Objekten und Attributen in einer einzigen Quelle. Federation stellen Verweise und Umleitungen auf Originalverzeichnisse dar, wenn die gesuchten Informationen nicht im Verzeichnis gefunden werden.

2.2.4 LDIF

Zum Datenaustausch mit dem LDAP-Verzeichnis können u.a. LDIF-Dateien benutzt werden. LDIF steht für LDAP Data Interchange Format. Diese Dateien sind ASCII-Dateien. Das Format wird durch RFC 2849 definiert und ist ein Standardformat für Textdateien, um LDAP-Konfigurationsinformationen und Verzeichnisinhalte aufzunehmen. Um ihren Inhalt in ein Verzeichnis übertragen zu können (z.B. unter Zuhilfenahme des Tools ldapmodify), müssen spezielle Formatierungsregeln eingehalten werden. Zum Beispiel ist die Verwendung von Leer- und Tabulatorzeichen genau geregelt. Durch diese Regelungen können Daten im Verzeichnis gefunden, bearbeitet und wieder zurück in das Verzeichnis übertragen werden. Außerdem können Objekte von einem Punkt im Verzeichnis an einen anderen kopiert bzw. verschoben werden. In seiner Grundform ist eine LDIF-Datei:

- Eine Sammlung von durch Leerzeilen voneinander getrennten Einträgen
- Eine Zuordnung von Attributnamen zu Werten
- Eine Sammlung von Direktiven, um anzuzeigen, wie Informationen zu verarbeiten sind

Um ein Objekt zu definieren und zu beschreiben, müssen in der LDIF-Datei folgende syntaktische Regeln eingehalten werden:

```
 [<Kennung>]
dn: <Distinguished Name>
<Attribut>: <Wert>
<Attribut>: <Wert>
<...> : <...>
```

Ein Objekt in der Datenbank besitzt immer eine eindeutige ID. Als Erstes haben Sie die Möglichkeit, eine Kennung für das Objekt anzugeben. Dies ist jedoch in der Praxis eher selten. In der nächsten Zeile wird der „Distinguished Name" des Objektes angegeben (Bsp.: `dn: dc=act,dc=de`). In den weiteren Zeilen werden die Attribute des Objektes definiert (Bsp.: `objectclass: organization`). Wenn Sie eine Datei mit mehreren Objekten erstellen, ist darauf zu achten, dass diese durch eine Leerzeile voneinander getrennt sind. In der Regel bestehen die Attributwerte aus druckbaren Zeichen, jedoch kann es auch vorkommen, dass binäre Daten abgelegt werden sollen.

```
# LDIF Eintrag fuer dn: dc=act,dc=de
dn: dc=act,dc=de
objectClass: domain
dc= act
```

Bei dem Erstellen von Dateien im LDIF-Format ist auf folgende Punkte zu achten (siehe Abbildung):

- Kommentare in einer LDIF-Datei beginnen mit einem # und gehen bis zum Ende der Zeile.
- Attribute werden links vom Doppelpunkt gelistet, deren Werte rechts davon. Vor dem eigentlichen Wert wird ein Leerzeichen gesetzt.

```
#-------------------------------------------------------------------------------
# Diese Datei wurde am 10.31.2004 um 17:40 aus ebel-dom.ebel:389
# mit LDAP-Browser 2.6 (http://www.ldapbrowser.com) erzeugt
#-------------------------------------------------------------------------------
version: 1
dn: CN=ACT-Web,OU=DE,O=ACT
objectclass: dominoServer
objectclass: top
dominocertificate:: MDMwMDMwMDIgQUM2OUU1RjAgMEJHMDE2MTYgRzAwMjhEMUIAQTFBQkFCMDMgRzAwMzAyMDAgMDEy
 MDg2MDAgNkQ0QjVCMDAAMOM2RjI1RzAgMDIORkcwMDIgNkUOQjVCMDAgMOI2RjI1MDAAQUVDOTYw
 MDAgMTY3MjI1MDAgMDFBMDc3MDAgNkQ0QjVCMDAAMOM2RjI1RzAgMDIORkcwMDIgNkUOQjVCMDAg
 MOI2RjI1MDAAQUVDOTYwMDAgMTY3MjI1MDAgNEY1NTNENDQgNDUyRjRGMOQANDEOMzUONDMgNEUz
 RDQxNDMgNTQyRDU3NjUgNjIyRjRGNTUAMOQONDQ1MkYgNEYzRDQxNDMgNTQOMjU2MDQgMDAzMTJF
 MzAAMDAOMjQzMDEgMDAwMzQyNDEgMDEwMDMwNDIgNEMwMjAwNzYAMDIORTRFNEYgMDA3RjQ5NkQg
 MzExMUI2MkIgMjkzRTkxNOUAMDBFMUFCRjcgMTc2NDQzRjcgQTZBQkVDOUEgQUUxMjUyOUYANjI4
 REUwRjggQOY3OTMOMDIgQUQOOTUyMDMgNDJENUIzQzcAODhFQTc1MjggMOMwRTgyMOIgODUzMOI2
 QTEgRjA5MDAOREEAMUQ2MENDNzIgNDMyMERGNDMgODQxNUJFOEUgMEJCMDczQkMAMEU4MDVFMzIg
 NDUORTAzMDAgMDEwMDAxNEQgNDEwODAwOTMAMjA3OUM4NDAgODQ2NTM3NOUgMDA1MDU1NTIgNTMO
 MTQ2NUMAMEFFREQ1NOMgMUI1OURGMTkgQzdEOTc1QkQgOTRERkYyMOYANzZDNjczNzMgRkY1RDRG
 MUIgRUNDODdBMOYgRjNGQTZDNkEAQjIzNDU2QjAgMDc1QUYORTAgOTMyQTAwOUEgMkFBMUY3QTAA
 MTIDOTAxMOEgQTYxQOM4QjYgRkYxMjBCNzIgMEQ4MUYxMEQANTQwNzc1MjEgMkFGQUIwMOQgRkUy
 QTdFODIgOTgxMDQyNTYAMDQwMDMxMkUgMzAwMDQyNDMgMDEwMDAzNDIgNDEwMTAwMzAANDIOQzAy
 RzAgMDEwMjRFNEUgNDAwMEFCNUEgNT1FMTg3QjkAOURFRURFRUIgOTVDREM3RTMgOTVEOTBBRjEg
 OEUxMDAOQOYAMjU4MkFEQjIgRDJFNkMzOUUgRUQ1MzVFRDQgMTkyOTc4MkYAQUJGOTkOQjAgODVG
 MjAyQkIgNTU3RUMwMzAgMjVDNTZBMUYAQTMxQzAxODcgODc5MjMwRDEgNUVDODQ1NEUgMDMwMDAx
 MDAAMDEORDQxMDggMDA1MUE5NEIgQzJGRTMwMEIgNEY2RjAwNTAANTU1MjUzNDEgNDYzRDg3ODUg
 NDcyNOJDNzkgRDc3MORBODMARTY1OTRDNDUgOURGNOEOODYgQUYzMzA2RjIgNUI5QUJDQTkANTE2
 MjgwRTcgMDQONEJEMzQgOUNDRDZEMEQgRjMyQORDMjUANzBDRDI3MDQgMEY3RUJEOTEgRDcwOTBC
 NOEgMDczOUYxREIAREIxNjY5MkIgRDAwNzIyRjEgNDBCQkJBOTkgMzgwMkNDMzIAODkOMUJBMjc=
creatorsname: CN=ACT-Web,OU=DE,O=ACT
modifiersname: CN=Nadin Ebel,O=ACT
createtimestamp: 200410291637117
modifytimestamp: 200410291807457
subschemasubentry: cn=schema
```

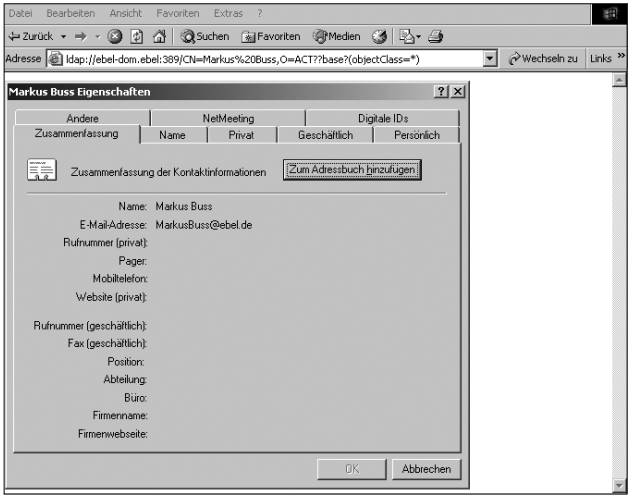
Textbasiert: Beispiel einer LDIF-Datei

- Der Wert wird durch einen Doppelpunkt hinter dem Attributnamen markiert.
- Bei der Angabe der Attributnamen wird nicht zwischen Groß- und Kleinschreibung unterschieden (objectClass = objectclass).
- Sollen die Daten in der LDIF-Datei zur Initialisierung eines Baumes verwendet werde, müssen die Objekte in der Baumstruktur, beginnend von der Wurzel, beschrieben werden. Es wird also der DN verwendet, der den Eintrag eindeutig identifiziert.

LDAP-URLs (RFC 1959):

```
<ldapurl> ::= "ldap://" [ <hostport> ] "/" <dn> [ "?"
➥ <attributes> [ "?" <scope> "?" <filter> ] ]
<hostport> ::= <hostname> [ ":" <portnumber> ]
<dn> ::= a string as defined in RFC 1485
<attributes> ::= NULL | <attributelist>
<attributelist> ::= <attributetype> | <attributetype> [ ","
➥ <attributelist> ]
<attributetype> ::= a string as defined in RFC 1777
<scope> ::= "base" | "one" | "sub"
<filter> ::= a string as defined in RFC 1558
```

LDAP-URLs definieren einen Standard, um sich auf Ressourcen im Internet bzw. Intranet zu beziehen. Sie werden u.a. in Verweisen (Referrals) verwendet, wie sie bei partitionierten Verzeichnissen vorkommen. Weiterhin dienen sie zur Angabe von Standardverweisen (References) auf übergeordnete Verzeichnisserver, falls eine Anfrage im lokalen Namensraum nicht erfüllt werden kann.



Abgefragt: Ergebnis eines LDAP-Aufrufs im Browser

LDAP-URLs finden auch Verwendung als Lesezeichen (Bookmarks). So ist es z.B. möglich, eine stets aktuelle E-Mailverteilerliste zu bekommen, indem eine Mailanwendung nicht die Empfänger der Liste, sondern eine Suchanfrage in Form einer LDAP-URL speichert und bei Bedarf diese Anfrage ausführt, um die einzelnen Empfänger zu ermitteln.

```
ldap[s]://[<host>:[<port>]][/
[<searchbase>[?[<attributes>][?[<scope>][?[<filter>]
➥ [?<extensions>]]]]]]
URL = "ldap://ldap.act-site.de/pfad/default.asp"
```

Die URL beginnt mit der Spezifikation des Protokolls: *ldap* für normale, ungesicherte Verbindungen bzw. *ldaps* für gesicherte, verschlüsselte Verbindungen, z.B. über SSL. Es folgt der Host-Name des LDAP Servers und optional der Port. Die Standards sehen Portnummer 389 für *ldap* bzw. 636 für *ldaps* vor. Die Angabe der Suchbasis ist trotz der eckigen Klammern, die optionale Teile kennzeichnen, bei den meisten LDAP-Servern nötig, um Ergebnisse zu erhalten. Die restlichen Argumente sind optional, wobei bei Auslassungen von Parametern die entsprechenden Fragezeichen zur Wahrung der Eindeutigkeit trotzdem anzugeben sind. Wird also z.B. die Angabe der Attribute und des Suchraumes (scope) ausgelassen und ein Filter angegeben, müssen drei Fragezeichen in Folge zwischen der Suchbasis (searchbase) und dem Filter angegeben werden.

2.2.5 LDAP und Sicherheit

Der Authentifizierungsprozess wird bei jedem Verbindungsversuch des Clients verwendet, um dessen Privilegien zu überprüfen und zu bestimmen. Alle Aktionen werden durch den Level der Autorisierung (Gewährung von Rechten) kontrolliert. Voraussetzung ist die erfolgreiche Authentifizierung. Generell stellen sich bei der Verwendung oder der Einführung von LDAP die folgenden Fragen, wie etwa:

- Welche Daten sollen im Verzeichnis gehalten und Bereitgestellt werden?
- Wer greift von wo aus auf das LDAP-Verzeichnis mit welchen Rechten zu?
- Wann erfolgen eine Verzeichnissynchronisierung und Maintenance-Arbeiten?
- Welche Rechte mit welchen Abstufungen benötigen die Benutzer und warum?
- Wie sieht die Unterscheidung in Bezug auf Schreib- und Lesezugriffe aus?
- Wer besitzt welche Rechte, um Verzeichnisinformationen zu aktualisieren?
- Welche Anwendungen arbeiten mit dem LDAP-Verzeichnis?

Zugriffssteuerung unter LDAP

Ein allgemein gültiges Konzept für die Zugriffskontrolle wurde anfänglich für LDAP nicht vorgesehen. Mittlerweile existieren jedoch über RFC 2820 einige allgemeine Empfehlungen in Bezug auf das Thema LDAP und Sicherheit. Alle we-

sentlichen LDAP-Implementierungen wie etwa OpenLDAP besitzen Mechanismen zur Zugriffssteuerung. Unter OpenLDAP kommen ACLs (Access Control List/Zugriffskontrollliste) zum Einsatz. Geregelt wird dies über die Konfigurationsdatei slapd.conf. Diese Datei enthält die Einträge für die Konfiguration des slapd Standalone Server. Der slapd beantwortet die LDAP-Anfragen der Clients – es ist der LDAP-Server oder Verzeichnisserver:

```
# User darf eigene Attribute ändern,
# authentifizierte User lesen
# alle andere sehen nichts
access to attr=telephoneNumber,seeAlso,description,audio,
    businessCategory,carLicense,displayName,homePhone,
    homePostalAddress,jpegPhoto,labeledURI,mobile,pager,
    photo,homeTelephoneNumber,favouriteDrink
  by self write
  by users read
  by * none
```

Oder so:

```
# Grundregel, damit anonyme User das Verzeichnis durchsuchen
➥ können
access to attr=entry,objectClass
by dn="uid=admin,ou=People,dc=Schriesheim,dc=int"
write
by * read
```

Oder so:

access to * attr=userPassword

```
        by self write
        by anonymous auth
access to *
        by * read
```

Die ACLs werden der Reihe nach abgearbeitet und die erste Übereinstimmung wird genommen. Im Beispiel kann ein beliebiger User das Passwort also nicht lesen. Zu beachten ist, dass der als rootdn definierte DN immer Schreiberlaubnis hat. In der schon bekannten BNF-Form würde dies so aussehen:

```
<access directive> ::= access to <what>
              [by <who> <access> <control>]+
<what> ::= * | [ dn[.<target style>]=<regex>]
              [filter=<ldapfilter>] [attrs=<attrlist>]
<target style> ::= regex | base | one | subtree | children
<attrlist> ::= <attr> | <attr> , <attrlist>
<attr> ::= <attrname> | entry | children
<who> ::= [* | anonymous | users | self |
      dn[.<subject style>]=<regex>]
      [dnattr=<attrname> ]
```

```
      [group[/<objectclass>[/<attrname>][.<basicstyle>]]
➥ =<regex> ]
      [peername[.<basic style>]=<regex>]
      [sockname[.<basic style>]=<regex>]
      [domain[.<basic style>]=<regex>]
      [sockurl[.<basic style>]=<regex>]
      [set=<setspec>]
      [aci=<attrname>]
<subject style> ::= regex | exact | base | one | subtree |
➥ children
<basic style> ::= regex | exact
<access> ::= [self]{<level>|<priv>}
<level> ::= none | auth | compare | search | read | write
<priv> ::= {=|+|-}{w|r|s|c|x}+
<control> ::= [stop | continue | break]
```

Dabei stellt `<what>` die Einträge und/oder Attribute dar, auf die der Zugriff gewährt wird, `<who>` spezifiziert, welchen Entities (`*`, `anonymous`, `users`, `self`, `dn=<regex>`) Zugriff gewährt wird und `<access>` bestimmt das Zugriffsrecht (`none`, `auth`, `compare`, `search`, `read`, `write`). Mehr Informationen zu dieser Thematik erhalten Sie z.B. unter www.openldap.org.

Authentifizierungsmechanismen

Bevor eine Zugriffssteuerung greifen kann, muss die Authentifizierung erfolgreich durchlaufen werden. Dieser Authentifizierungsprozess existiert seit den frühesten LDAP-Versionen. In der Terminologie von LDAP spricht man von einer Bindung an das Verzeichnis. Benötigte Parameter für eine Bindung sind der Benutzername in Form eines DN und ein Passwort (Credential). Zur Erfüllung verschiedener Ansprüche an die Sicherheitsstufen gibt es folgende grobe Einteilung der Authentifizierung:

- Keine Authentifizierung wird beispielsweise verwendet bei öffentlich lesbaren Verzeichnissen. Durch Übergabe eines leeren Benutzernamens und eines leeren Passwortes kann ein LDAP-Client eine anonyme Anmeldung erfragen.
- Bei der normalen Authentifizierung (Basic Authentication) wird der Benutzer durch den Benutzernamen in Form eines DNs und ein Klartext-Passwort gegenüber dem Verzeichnisdienst identifiziert. Diese Variante bietet keinen Schutz gegen das Abhören und den Missbrauch der übermittelten Daten im Netzwerk.
- Die sichere Authentifizierung bietet durch die Implementierung von SASL (Simple Authentication and Security Layer, RFC 2222) ein erweiterbares Framework zur Authentifizierung. Verschiedene Sicherheitsmethoden wie Kerberos, S/Key oder SSL/TLS (Secure Sockets Layer/Transport Layer Security) lassen sich einbinden. Bei Verwendung entsprechender Sicherheitsmodule wie beispielsweise SSL ist eine beidseitige verschlüsselte Authentifizierung mit anschließendem verschlüsselten Datenverkehr möglich. Bei Sicherheitsme-

thoden, die auf Public-/Private-Key-Algorithmen basieren, lassen sich die benötigten Zertifikate sinnvollerweise im LDAP-Verzeichnis ablegen.

Verwendung findet dieses Authentifizierungsverfahren hauptsächlich bei der Kommunikation zwischen Verzeichnisservern. Die übertragenen Daten einer Replikation sind oftmals sicherheitskritisch. Außerdem wird meist umfassender schreibender Zugriff auf die Replik benötigt, der für andere Anwendungen verhindert werden soll.

Durch RFC 2251 ist der Authentifizierungsprozess für LDAP definiert worden. Es handelt sich um die so genannte Bind-Operation (Bindung), mittels derer sich ein LDAP-Client beim LDAP-Server anmeldet. Diese Operation ist in ein Bind Request und ein Bind Response aufgeteilt. Der bind request enthält neben der LDAP-Protokollversionsnummer einen DN eines Eintrags, welcher die zu beweisende Identität kennzeichnet, also z.B. ein Personeneintrag, sowie schließlich die Kennzeichnung der verwendeten Authentifizierungsmethode und die dazugehörenden Daten. Hierbei sind zurzeit zwei Methoden definiert:

- Simple Bind: Hierbei wird zusätzlich zum DN ein Passwort mitgeschickt. Dieses wird vom Server mit dem im DN bezeichneten Eintrag gespeicherten Passwort verglichen. Da das Passwort ungeschützt über das Netz geschickt wird, also jederzeit abgehört werden kann, wird von der Verwendung von Simple Bind ohne vorherige Verschlüsselung der Verbindung abgeraten. Eine solche Verschlüsselung ist jedoch mit TLS möglich und ebenfalls im Standard spezifiziert. Simple Bind wird auch für anonymen Zugriff auf LDAP-Verzeichnisse verwendet, wobei sowohl der DN als auch das Passwort leer bleiben. Alternativ kann bei anonymem Zugriff auch ganz auf die bind-Operation verzichtet werden.
- SASL Bind: SASL (Simple Authentication and Security Layer) ist ein IETF-Standard (RFC 2222), mit dem der Authentifizierungsvorgang von der eigentlichen Anwendung in einer eigenen Schicht gekapselt wird, so dass nicht für jedes Anwendungsprotokoll ein eigener Authentifizierungsmechanismus definiert werden muss. Neben einer Reihe von verschiedenen Authentifizierungsmechanismen wird in SASL auch eine optionale Verschlüsselung der Verbindung zur Verfügung gestellt.

Folgende SASL-Mechanismen wurden entweder in RFC 2222 oder in Folgespezifikationen definiert:

- PLAIN, ein einfacher Passwortmechanismus, der nicht besser ist als das simple bind.
- KERBEROS_V4, wobei Kerberos Version 413 verwendet wird, welches jedoch wegen einiger Sicherheitsmängel als obsolet zu betrachten ist. Kerberos ermöglicht Single Sign-On (SSO), also einen einmaligen Authentifizierungsprozess, der für mehrere Authentifizierungsvorgänge gültig ist, da einem Client als Authentifizierungsnachweis ein so genanntes Kerberos Ticket ausgestellt wird, welches eine bestimmte Gültigkeitsdauer hat und automatisch an Kerberos-fähige Anwendungen übermittelt wird.

- GSSAPI, ein SASL-Mechanismus, der wiederum eine eigene (GSSAPI genannte) gekapselte Schnittstelle verwendet, durch die eine Reihe von weiteren Authentifizierungsmechanismen zur Verfügung gestellt werden.

GSSAPI steht für Generic Security Service Application Program Interface (Version 2 in RFC 2078). Die beiden wichtigsten GSSAPI-Mechanismen sind:

Kerberos V5 (RFC 1510), eine Kerberosversion, in der die Sicherheitsschwächen von Kerberos V4 behoben wurden.

X.509-basierte so genannte Strong Authentication, bei der die Authentifizierung über X.509-Schlüsselpaare in Verbindung mit der Zertifizierung des öffentlichen Schlüssels geschieht. Über die „Hintertür" GSSAPI wird so das für X.500 spezifizierte strong bind ermöglicht.

- DIGEST MD5 (RFC 2831), ein SASL-Mechanismus, der auf dem MD5-Hash-Algorithmus (RFC 1321) beruht, bei dem in einem Challenge-Response-Verfahren der Server einen Zufallstext an den Client schickt. Dieser errechnet einen auf diesem Text und das Passwort basierenden Hash, den er an den Server zurückschickt. Dieser berechnet ebenfalls den Hash und kann dadurch feststellen, ob der Client im Besitz des richtigen Passwortes ist, ohne dass dieses über das Netz geschickt werden musste.
- EXTERNAL, ein SASL-Mechanismus, bei dem eine bereits auf unteren Protokollschichten (z.B. via X.509) etablierte gesicherte Verbindungen auf der Transportschicht mittels IPSec (RFC 2401) oder auf der Sessionschicht mittels SSL/TLS (RFC 2246) etablierte Authentifizierung für die Anwendungsschicht verwendet wird.

Abhängig vom gewählten SASL-Mechanismus werden bei der LDAP-Authentifizierung im bind request anstelle des DNs andere Identitätskennungen (z.B. ein Kerberos-principle) und andere Identitätsbeweise mitgeschickt. Ebenfalls abhängig vom Authentifizierungsmechanismus schickt der Server als Antwort unterschiedlich modellierte bind responses zurück. Der hierbei mitgegebene Error-Code (SUCCESS, wenn die Authentifizierung erfolgreich war, oder aber der Grund, warum diese nicht erfolgreich war) ist jedoch in jedem Fall festgelegt.

In RFC 2830 wird spezifiziert, wie TLS zur Verschlüsselung der gesamten Kommunikation zwischen Client und Server im LDAP-Protokoll verwendet werden soll. Hierbei initiiert der Client eine solche Verschlüsselung durch den StartTLS-Befehl, wonach die zu verwendende TLS/SSL-Version ausgehandelt wird sowie die X.509-Zertifikate ausgetauscht werden. Mit TLS kann sich nicht nur der Server mit seinem Zertifikat authentifizieren, sondern auch der Client. In diesem Fall kann die Client-Authentifizierung über den SASL-Mechanismus EXTERNAL auch für die LDAP-Authentifizierung verwendet werden. Ansonsten dient TLS nur zur Verschlüsselung der Verbindung. RFC 2829 spezifiziert, welche dieser Authentifikationsmechanismen von einer standardkonformen LDAPv3-Implementierung in jedem Fall unterstützt werden muss:

- Anonyme Authentifizierung (keine Authentifizierung oder simple bind mit leerem Passwort)
- Passwortauthentifizierung mittels des SASL-Mechanismus DIGEST MD5
- Durch TLS geschützte Passwortauthentifizierung mittels simple bind oder TLS-geschützte Authentifizierung per SASL-Mechanismus EXTERNAL

Viele LDAP-Implementierungen unterstützen aber mehr als diese drei Pflichtmechanismen. So lässt sich zum Beispiel mit der Open-Source-Implementierung OpenLDAP eine Authentifizierung mittels Kerberos 5 via SASL-GSSAPI realisieren. Welche SASL-Mechanismen ein Server unterstützt, wird in einem speziellen Eintrag, dem so genannten ROOTDSE-Eintrag, veröffentlicht.

Passwörter können in LDAP-Servern sowohl im Klartext als auch verschlüsselt abgelegt werden. Das Standard-Schema spezifiziert zur Speicherung des Passworts das Attribut USERPASSWORD. Wird es verschlüsselt abgelegt, wird der jeweilige Verschlüsselungs- bzw. Hash-Algorithmus in geschwungener Klammer vor das verschlüsselte Passwort gesetzt. Die üblichsten Algorithmen sind crypt, md5 und sha, aber auch die sichereren smd5 und ssha können eingesetzt werden. Damit der Client beim Setzen eines neuen Passworts nicht wissen muss, wie der Server das Passwort ablegt, wurde in RFC 3062 eine Erweiterung des LDAP-Protokolls spezifiziert. Bei manchen Authentifizierungsverfahren über SASL werden die Passwörter auch gar nicht im LDAP-Server, sondern an anderen Orten gespeichert (RADIUS).

Die Erweiterung bewirkt, dass der Server das vom Client mit dem alten Passwort zusammen geschickte neue Passwort entsprechend seiner Konfiguration verarbeitet und speichert. Des Weiteren wurde in RFC 3112 ein neues Attribut AUTHPASSWORD mit einer eigenen Syntax für verschlüsselte Passwörter spezifiziert.

Sicherheitsrisiken bei der Verwendung von LDAP

Beim Einsatz eines zentralen Authentifizierungssystems wird die Kompromittierung des zentral gespeicherten Passworts zu einem erhöhten Sicherheitsrisiko. Wenn dieses zentrale Passwort kompromittiert wurde, ist eben nicht nur ein Rechner oder eine Anwendung offen, sondern alle Schnittstellen, die am Authentifizierungssystem angeschlossen sind. Daher sollten root-Passwörter immer dezentral auf den jeweiligen Rechnern bleiben und nicht in das LDAP-Authentifizierungssystem integriert werden.

Es gibt mittlerweile eine ganze Reihe von Hackertools, deren dediziertes Ziel ist, LDAP-Passwörter zu kompromittieren. Eines dieser Tools ist das C-Programm Kold („Knocking on LDAP's Door“ http://www.phenoelit.de), welches einen Wörterbuch-Angriff auf jeden Eintrag eines LDAP-Servers durchführt. Ein Perl-Programm mit ähnlicher Funktion heißt LDAP_Brute.pl (http://angreypacket.com). Solche Online-Attacken sind relativ leicht an den Log-Dateien des LDAP-Servers zu erkennen. Darüber hinaus setzen sie voraus, dass entweder anonym auf den LDAP-Server zugegriffen werden kann oder dass dem Angreifer mindestens ein Passwort bekannt ist, um überhaupt die Einträge finden zu können. Schließlich

funktionieren solche Attacken auch nur bei sehr schwachen Passwörtern, die aus Vornamen oder ganzen Wörtern bestehen. Wenn darauf geachtet wird, dass z.B. mindestens eine Ziffer und ein Sonderzeichen im Passwort enthalten sind, gehen solche Angriffe meistens ins Leere. Adäquate Passwortqualität ist also gefordert.

Ein weiteres Tool zum Kompromittieren von LDAP-Passwörtern heißt Lumberjack (http://www.phenolit.de), welches nicht einen LDAP-Server angreift, sondern LDIF-Dateien analysiert. LDIF-Dateien werden häufig zu Replikationszwecken über das Netz geschickt und können – geschieht dies nicht durch verschlüsselte Kanäle – abgefangen werden. Es wurde sogar beobachtet, dass Firmen solche LDIF-Dateien offen im Web abgelegt hatten. Lumberjack versucht, die verschlüsselten Passwörter in LDIF-Dateien zu knacken. Da der Angriff nicht über das Netz geht – der Angreifer also unbegrenzte Zeit für die Analyse hat –, versucht Lumberjack jede mögliche Kombination aus Buchstaben, Ziffern und Sonderzeichen, verschlüsselt diese mit dem in geschwungener Klammer angegebenen Algorithmus und vergleicht das Resultat mit den verschlüsselten Passwörtern. Aufgrund der Existenz solcher Tools wie Lumberjack ist von einer Klartextübertragung von LDIF-Dateien unbedingt abzuraten. Außerdem sollte darauf geachtet werden, dass die Passwörter in kurzen Abständen erneuert werden.

Ein wesentliches Merkmal für sichere Passwörter ist die Kontrolle der Passwortlänge, der Nutzung eines möglichst großen Zeichenvorrats (Klein- und Großbuchstaben, Ziffern und Sonderzeichen) bei der Bildung von Passwörtern, ihrer Gültigkeitsdauer und der Beschränkung ihrer Wiederverwendung. Eine diese Punkte vorschreibende Passwortregel (Password Policy) ist gerade im Zusammenhang mit zentralen Authentifizierungssystemen von großer Bedeutung. Viele LDAP-Implementierungen können solche Regeln erzwingen.

Ein entsprechender Standard wird zurzeit im Rahmen der IETF entwickelt. Für LDAP-Implementierungen, wie die Open-Source-Implementierung OpenLDAP, die bisher solche Passwortregeln nicht unterstützen, kann diese Funktionalität mittels eines Web-Front-Ends implementiert werden. Dabei muss aber sichergestellt sein, dass Passwortänderungen nur über dieses Gateway erfolgen. Außerdem muss zusätzlich ein Client regelmäßig überprüfen, ob Passwörter bereits abgelaufen sind und solche Einträge dann entsprechend sperren.

Wie bei allen anderen Netzwerkprotokollen, bilden Angriffsszenarien, wie „Man in the Middle Attack“ und das Abhören von Netzverbindungen weitere mögliche Gefahren. Das Ziel eines solchen Angriffs ist es, den Computer des Angreifers logisch zwischen den beiden kommunizierenden Computern zu postieren, um den gesamten Datenverkehr zu kontrollieren. Abhilfe bringen bei einem solchen Szenario digitale Signaturen. Wenn für die LDAP-Kommunikation, insbesondere beim Authentifizierungsvorgang, TLS verwendet wird, sollten aber auch solche Angriffe nicht fruchten. Während der Initiierung einer TLS-Verbindung kann sowohl eine Server- als auch eine Client-Authentifizierung mittels X.509-Zertifikaten durchgeführt werden, wodurch auch „Man in the Middle“-Angriffe ausgeschlossen werden können.

2.2.6 LDAP in der Anwendung

LDAP kommt in den unterschiedlichsten Bereichen und Funktionen zur Anwendung. Der Umfang verzeichnisartiger Informationen nimmt in starkem Maße zu. Nachteilig ist, dass diese Informationen oftmals in verschiedenen proprietären Datenbanken abgelegt sind. LDAP bietet ein flexibles, einfach zu handhabendes Standardprotokoll zur Verwaltung all dieser Informationen. Die direkte Integration von LDAP-Unterstützung in die Client-Programme vereinfacht die Umstellung bzw. das Neuprogrammieren von Verzeichnisdienst-Clients.

Außerdem lassen sich die Verwaltungsdaten von Betriebssystemen auf LDAP-Servern ablegen, sofern die Betriebssysteme ausreichend modular gestaltet sind. Derzeit ist es z.B. unter Linux und Solaris dank PAM (Pluggable Authentication Module) bzw. NSS (Name Service Switch) möglich, die gesamte Benutzerverwaltung im Verzeichnis zu halten und zu pflegen. Verschiedene Daemon-Software wie der sendmail-MTA, der Apache-Webserver oder Samba können ebenfalls ihre Benutzerverwaltungstabellen aus LDAP-Verzeichnissen beziehen. Auch ausgewachsene Systems Management-Software wie Tivoli oder HP OpenView gewinnen durch den Einsatz von LDAP-Verzeichnissen an Flexibilität.

Authentifizierung/Systemverwaltung

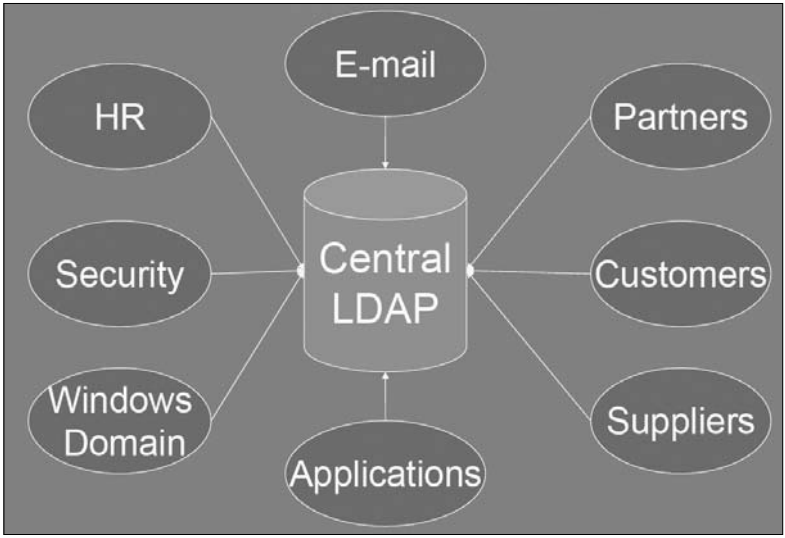
Ein großes Anwendungsgebiet für LDAP sind Authentifizierungen. Hier liegen die Benutzerinformationen wie Username und Passwort im Verzeichnis. So kann das System den Benutzer gegen das Verzeichnis authentifizieren. Dies gilt übrigens nicht nur für die verschiedenen Unix-Plattformen, sondern zum Beispiel auch für die Regelung des Zugangs zu Webseiten.

Die Einsatzmöglichkeiten für die elektronische Authentifizierung sind vielfältig. Ein entsprechendes Verfahren kann prinzipiell in jede Client-Server- oder Multi-Tier-Anwendung integriert werden, um den Clients oder auch einzelnen Anwendern den Zugriff auf die entsprechenden Systemkomponenten zu gewährleisten. Darüber hinaus lassen sich mithilfe einer elektronischen Authentifizierung auch komfortable Single Sign-On-Lösungen realisieren, d.h., ein Anwender meldet sich einmalig bei einer bestimmten Serverkomponente (z.B. LDAP-Verzeichnis) an und bekommt dabei die seiner Rolle entsprechenden Rechte zugewiesen. Ab diesem Zeitpunkt hat der Anwender die Möglichkeit, auf weitere Anwendungen – zu deren Nutzung er berechtigt ist – zuzugreifen, ohne sich bei jeder genutzten Anwendung neu anmelden (authentifizieren) zu müssen (siehe Abbildung 3.13). Ein denkbares Szenario ist die einmalige (morgendliche) Anmeldung eines Anwenders an seinem Arbeitsplatz-PC, danach hat er Zugang zum Intranet, Internet und dezidierten Anwendungssystemen (z.B. SAP, FIBU, MIS), ohne weitere Benutzernamen und/oder Passwörter eingeben zu müssen.

Zudem kommt LDAP vermehrt zur Anwendung im Bereich der Mailserver (Adressbuch), zur Authentifizierung, zur Speicherung ihrer Konfigurationen und zur Abfrage von Empfängern.

Identity Management

Als Speicherort aller Informationen über die gemanagten Identitäten dient in der Regel ein LDAP-Verzeichnis (siehe Abbildung).



Multifunktional: Beispiel einer LDAP-Anwendung in Unternehmen

Adressbuch

Als Adressbuch findet LDAP häufiger Verwendung, beispielsweise zum Einbinden von Benutzerdaten in Webseiten oder als unternehmensweites Adressbuch mit Schnittstelle zu den Mailprogrammen. Praktisch hierbei ist, dass die Informationen des Benutzerverzeichnisses verwendet werden können, so dass ein Benutzer einmal angelegt wird und dann auch sofort in allen Adressbüchern auftaucht. Gleichzeitig können die Informationen des Benutzerverzeichnisses für die Authentifizierung verwendet werden.

2.2.7 LDAP-Tools

An dieser Stelle werden die Befehle von OpenLDAP unter Linux vorgestellt.

Die wichtigsten LDAP-Tools sind:

ldapsearch – Suchen im LDAP-Verzeichnis

Das Programm ldapsearch dient dazu, nach Attributen oder Werten von Attributen im Verzeichnisbaum zu suchen. Der Output von ldapsearch entspricht in der Syn-

tax einem LDIF-File. So kann dieser Output direkt wieder verwendet werden, um zum Beispiel Daten von einem Teil des LDAP-Baums in einen anderen zu kopieren. Unter Lotus Domino und im IBM Directory Server ist ldapsearch standardmäßig implementiert.

ldapadd – Hinzufügen von Einträgen in das LDAP-Verzeichnis

ldapmodify – Ändern von Einträgen im LDAP-Verzeichnis

ldapdelete – Löschen von Einträgen im LDAP-Verzeichnis

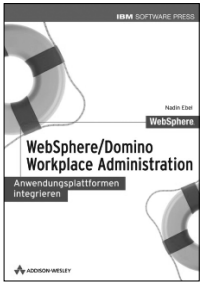
Die Programme ldapadd und ldapmodify sind identisch. Bei ldapadd wird ldapmodify lediglich mit dem Parameter HINZUFÜGEN aufgerufen. Mit ldapmodify lassen sich Änderungen an Objekten im LDAP-Baum durchführen. Dazu bietet ldapmodify zwei Möglichkeiten: Entweder tippt man die Informationen in der Kommandozeile ein oder erstellt zunächst eine LDIF-Datei und übergibt diese dann an ldapmodify.

ldapmodrdn – Umbenennen von Einträgen im LDAP-Verzeichnis

ldappasswd – Ändern von Benutzerpasswörtern im LDAP-Verzeichnis. (mha)

Weiterführende Infos

Die Artikelserie „LDAP“ basiert auf dem Kapitel 3 des Standardwerks „Websphere/Domino Workplace Administration“ von IBM Software Press aus dem Addison-Wesley Verlag (http://www.addison-wesley.de/). Sie können dieses 900 Seiten starke Buch auch in unserem Buchshop (http://www.tecchannel.de/abo+shop/buchshop/) bestellen oder als eBook herunterladen.



tecCHANNEL-Links zum Thema	Webcode	Compact
LDAP	438638	S.90
Katastrophenszenarien Active Directory	434994	S.177

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

2.3 Katastrophenszenarien bei Active Directory

Active Directory ist auf eine Reihe von Diensten und Features angewiesen, um korrekt funktionieren zu können. Wenn einer dieser Dienste ausfällt, erleben Sie ungewöhnliches oder unkontrollierbares Verhalten. In diesem Kapitel werden die folgenden Problemszenarien besprochen:

- DNS-Server-Ausfall und Auswirkungen auf Clients und Domänencontroller
- Ausfall eines Domänencontrollers, inklusive Verlust von Global Catalog Servern und FSMO-Rollenmastern
- Ausfall von zentralen Replikationskomponenten wie Brückenkopf-Server, ISTGs und WAN-Leitungen
- Verlust oder Beschädigung der Active Directory-Datenbank und Methoden zur Sicherung und zum Wiederherstellen der Datenbank
- Kein Problemszenario, aber inhaltlich verwandt: Active Directory-Pflege, wie etwa Entfernen von ESE-Dateien für alternative Speicherorte, Defragmentierung der AD-Datenbank und Festlegung der AD-Konfigurationsparameter

Nach diesem Artikel sind Sie mit bewährten Methoden vertraut , wie Sie Active Directory im laufenden Betrieb pflegen und im Notfall wiederherstellen können.

2.3.1 Neue Features von Windows Server 2003

Das einzige neue Feature von Windows Server 2003, das sich auf Active-Directory-Ausfälle und -Korrektur auswirkt, ist die neue Fähigkeit von Domänencontrollern, die keine GC-Server sind, Mitgliedschaften in universellen Gruppen zu cachen. Der Global Catalog (GC) speichert die Mitgliedschaftslisten für universelle Gruppen, und ohne diese Information verweigert ein Domänencontroller Benutzern die Authentifizierung. Normalerweise würde ein Zusammenbruch der Verbindung zu GC-Servern (beispielsweise nach dem Ausfall einer Standleitung) dazu führen, dass Benutzer sich nicht mehr an der Domäne anmelden können. Da nun Mitgliedschaft in universellen Gruppen auf normalen Domänencontrollern gecacht wird, würde der Ausfall der Verbindung zu den Global Catalogs nicht mehr zum Abschneiden von der Domäne führen.

2.3.2 Ausfall eines DNS-Servers

Der Ausfall eines DNS-Servers wirkt sich in mehrerlei Hinsicht auf Active Directory aus. Erstens muss ein Domänencontroller in der Lage sein, Hostnamen und Server-Einträge aufzulösen, um mit den anderen Domänencontrollern kommunizieren und replizieren zu können.

Wenn der DNS-Server ausfällt, den ein Domänencontroller benutzt, dann kann der DC seine Funktionalität nicht mehr lange voll aufrechterhalten.

Sie müssen Ihre DNS-Infrastruktur so gestalten, dass der Ausfall eines einzelnen DNS-Serves nicht zu einer Betriebsunterbrechung führt. Sie sollten stets mindestens zwei DNS-Server betreiben, die für eine Zone autoritativ sind, und die Clients sollten auf beide Server verweisen, auf den einen als primären, den anderen als sekundären DNS-Server. Windows-Clients wenden sich an ihren sekundären DNS-Server, wenn sie vom primären DNS-Server keine Antwort erhalten.

Inseleffekt vermeiden

Wenn Sie einen Domänencontroller, der ein DNS-Server mit AD-integrierten Zonen ist, für die Namensauflösung auf sich selbst verweisen lassen, könnten Sie einem subtilen Teufelskreis zum Opfer fallen, den Microsoft als Inseleffekt bezeichnet. Bei einer AD-integrierten DNS-Zone aktualisiert ein Domänencontroller seine DNS-Einträge, indem er von einem anderen Domänencontroller repliziert. Der Domänencontroller findet seine Replikationspartner, indem er einen DNS-Lookup durchführt. Wenn sich IP-Adressen ändern, findet der Domänencontroller seinen Replikationspartner nicht und kann DNS nicht aktualisieren, weil er nicht von ihm replizieren kann.

Sie können diesen Inseleffekt vermeiden, indem Sie die TCP/IP-Eigenschaften eines Domänencontrollers so konfigurieren, dass ein anderer Domänencontroller der primäre DNS-Server ist. Die DNS-Einstellungen in den TCP/IP-Einstellungen des Domänencontrollers können auf den Domänencontroller selbst als sekundären DNS-Server verweisen, denn schließlich sollte der sekundäre Eintrag nur kurzfristig im Ausnahmefall gebraucht werden.

Folgen eines DNS-Ausfalls für Windows-Clients

Ohne DNS können Active Directory Clients keine SRV-Einträge finden, die sie für das Auffinden der Domänencontroller benötigen. Die Clients können sich ohne diese Einträge nicht authentifizieren oder LDAP-Abfragen durchführen.

Nach dem Verlust der DNS-Server funktionieren die Clients zunächst weiter, indem sie gecachte DNS-Einträge verwenden. Der SOA-Eintrag für die DNS-Domäne legt fest, wie lange die Standardgültigkeit (TTL, Time-To-Live) für DNS-Einträge ist, die von den Nameservern der Zone kamen. Die voreingestellte TTL für Windows-DNS ist 1 Stunde (3600 Sekunden).

Wenn die SRV-Einträge abgelaufen und die DNS-Server immer noch nicht verfügbar sind, finden die Clients ihre Domänencontroller nicht mehr. Sie können Ihre Kerberos-Sitzungstickets nicht mehr erneuern und können sich daher nicht mehr mit Mitgliedsservern verbinden.

Bei der Planung Ihrer DNS-Infrastruktur sollten Sie stets einen Ersatz-DNS-Server an jeder Niederlassung einplanen. Das kann ein normaler sekundärer Nameserver oder ein Domänencontroller mit Active-Directory-integrierter Zone sein.

2.3.4 Ausfall eines Domänencontrollers

Wenn ein Domänencontroller ausfällt, merkt dies der Kerberos-Dienst auf den Clients, wenn die lokal gecachten Kerberos-Tickets ablaufen und der Kerberos-Dienst versucht, sie zu erneuern. Sobald der Client merkt, dass sein Anmeldeserver nicht antwortet, fragt er DNS nach anderen Domänencontrollern und benutzt einen von ihnen für die erneute Authentifizierung. Der Benutzer merkt nichts davon. Falls der ausgefallene Domänencontroller (DC) der einzige Controller am Standort war, müssen sich die Clients über WAN neu authentifizieren. Das verlangsamt die Authentifizierung je nach Geschwindigkeit der Anbindung. Während der lokale DC nicht verfügbar ist, dauern LDAP-Anfragen wie eine Suche nach Druckern oder die Verwendung von Outlook in einer Exchange 2000-Umgebung wegen der WAN-Leitungslatenz länger.

Sollten keine anderen DCs zur Reauthentifizierung zur Verfügung stehen, verfallen irgendwann die Kerberos-Tickets des Clients, und er verliert die Verbindung zu Mitgliedsservern. Wenn sich die Clients abmelden, können sie sich mit gecachten Anmeldedaten wieder anmelden, doch die gecachten Anmeldedaten erlauben keinen Zugriff auf Mitgliedsserver.

Merken Sie sich also, dass eine unterbrochene WAN-Leitung den Zugriff auf lokale Windows-Server beendet, falls es keine lokalen Domänencontroller gibt. Sie könnten eine Ersatz-WAN-Anbindung einrichten, beispielsweise eine ISDN-Leitung, die nur anspringt, wenn die Hauptanbindung unterbrochen ist. Alternativ können Sie einen lokalen Domänencontroller installieren. Der muss dann, wie wir im nächsten Abschnitt sehen werden, entweder ein GC-Server oder aber so konfiguriert sein, dass er Global Catalog Einträge cacht.

Ohne Global Catalog anmelden

Normalerweise können sich Benutzer nicht an einer Domäne anmelden, wenn kein Domänencontroller verfügbar ist, der eine Kopie des Global Catalog besitzt. Der Grund hierfür ist, dass der GC die Mitgliedschaftsliste für universelle Gruppen hostet. Außerdem: Wenn sich Benutzer mit dem UPN anmelden (Benutzer@Firma.de), dann wird ein GC benötigt, um den UPN in seine Bestandteile zu zerlegen. Windows XP cacht den zerlegten Namen nach dem ersten Anmelden, doch Windows 2000 braucht bei jedem erneuten Anmeldevorgang per UPN einen Global Catalog.

Bei Windows Server 2003 können nun normale Domänencontroller die Mitgliedschaft in universellen Gruppen cachen. Das erlaubt solchen Domänencontrollern, Benutzer zu authentifizieren, wenn der GC nicht erreicht werden kann. Der Cache für die Mitgliedschaft in universellen Listen macht einen Domänencontroller nicht zum GC-Server. Der cachende Domänencontroller lauscht nicht auf LDAP-Anfragen auf Port 3268, und er hostet keine Objekte aus anderen Domänen, wenn man von Mitgliedschaft in universellen Gruppen absieht. Das Cachen universeller Gruppen erfordert keine zusätzlichen Prozessoren oder mehr RAM bei den Do-

mänencontrollern am Standort. Wenn aktiv, wird dieser Cache alle acht Stunden aktualisiert. Wurde ein Benutzer nach der letzten Aktualisierung einer universellen Gruppe hinzugefügt, werden die Berechtigungen, die zu dieser Gruppe (und allen Gruppen, denen diese Gruppe angehört) gehören, nicht in das PAC des Benutzers geschrieben. Sie sind daher auch nicht Bestandteil lokaler Zugriffstoken, die für den Benutzer auf Mitgliedsservern erzeugt werden. Der Cache für Mitgliedschaften in universellen Gruppen kann ungefähr 500 Gruppen speichern.

Sie sollten das Cachen von Mitgliedschaften in universellen Gruppen an jedem Standort aktivieren, wo kein GC-Server steht. Gehen Sie dazu wie folgt vor:

Das Cachen von Mitgliedschaften in universellen Gruppen aktivieren

1. Öffnen Sie die Konsole ACTIVE DIECTORY-STANDORTE UND -DIENSTE.

2. Markieren Sie den Standort, den Sie konfigurieren wollen.

3. Im rechten Teil öffnen Sie das Fenster Eigenschaften des Objekts NTDS SITE SETTINGS (siehe Bild 1).

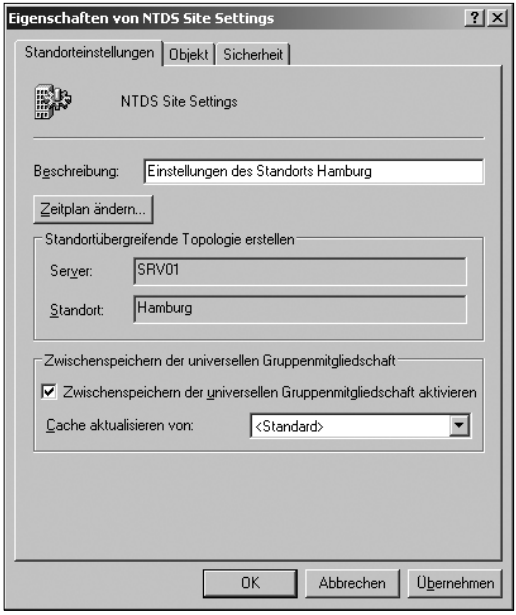


Bild 1: Eigenschaften von NTDS Site Settings mit der Option für das Zwischenspeichern universeller Gruppenmitgliedschaften.

4. Wählen Sie ZWISCHENSPEICHERN DER UNIVERSELLEN GRUPPENMITGLIEDSCHAFT AKTIVIEREN. Ändern Sie CACHE AKTUALISIEREN VON nicht. Der KCC findet den nächsten Standort mit einem GC-Server.

5. Klicken Sie auf OK, um die Änderung zu speichern und das Fenster zu schließen.

Metadaten für einen verlorenen Domänencontroller löschen

Wenn Sie einen ausgefallenen Domänencontroller überhaupt nicht mehr zum Laufen bekommen, müssen Sie die Referenzen auf ihn aus Active Directory löschen. Diese so genannten Metadaten müssen gelöscht werden, ehe Sie einen anderen Server mit demselben Namen zu einem Domänencontroller hochstufen können. Sollten Sie gar eine ganze Domäne verlieren, so müssen Sie gleichfalls die Metadaten-Information für die Domäne entfernen, bevor Sie eine gleichnamige Domäne neu erstellen können. Das Werkzeug für Entfernen der Metadaten ist ein Kommandozeilentool namens Ntdsutil. Das Löschen erfolgt im laufenden Betrieb von Active Directory. Verwenden Sie dazu diese Schrittfolge:

1. Starten Sie `Ntdsutil`.

2. Geben Sie an der Eingabeaufforderung Ntdsutil: den Befehl metadata cleanup ein, um die gleichnamige Eingabeaufforderung zu öffnen.

3. Geben Sie ? ein, um die Liste der Optionen anzuzeigen:

Ntdsutil-Optionen	
?	Zeigt diese Hilfeinformationen an
Connections	Verbindung mit einem bestimmten Dömänencontroller herstellen
Help	Zeigt diese Hilfeinformationen an
Quit	Zum vorherigen Menü wechseln
Remove selected domain	DS-Objekte für die gewählte Domäne entfernen
Remove selected Naming Context	Entfernen Sie die DS-Objekte für den gewählten Namenskontext
Select operation target	Standorte, Server, Domänen, Funktionen und Namenskontexte wählen

4. Geben Sie `connections` und dann ? für eine Liste der Optionen ein.

Ntdsutil-Optionen	
Clear creds	Frühere Verbindungsinformationen löschen
Connect to domain %s	Verbindung mit Server, DNS-Namen oder IP-Adresse herstellen
Connect to server %s	Verbindung mit Server, DNS-Namen oder IP-Adresse herstellen

Help	Zeigt diese Hilfeinformationen an
Info	Verbindungsinformationen anzeigen
Quit	Zum vorherigen Menü wechseln
Set creds %s %s %s	Verbindungsinformationen als Domäne, Benutzer und Kennwort festlegen (Verwenden Sie „NULL“ für ein Null-Kennwort, * um das Kennwort von der Konsole einzugeben)

5. Wenn Sie an einem Mitgliedsserver arbeiten und nicht mit Administratordaten angemeldet sind, verwenden Sie den Befehl `set creds`, um Ihre Verbindungsinformationen angeben zu können.

6. Geben Sie connect to server <dsa> ein, um sich mit einem Server zu verbinden. Hierbei ist <dsa> der vollqualifizierte DNS-Name des DC, auf dem Sie die Verzeichnisveränderung vornehmen wollen. Das geht bei jedem funktionsfähigen Domänencontroller. Die Einträge und Transaktionsergebnisse sehen bis zu dieser Stelle wie folgt aus:

```
server connections: set creds firma.de administrator passwort
server connections: connect to server srv01.firma.de
Bindung mit "srv01.firma.de" als firma.de\administrator...
Verbindung mit "srv01.firma.de" als firma.de\administrator.
```

7. Geben Sie erst `quit`, dann `select operation target` ein, um die gleichnamige Eingabeaufforderung zu öffnen. Rufen Sie über `?` die Optionsliste auf:

Optionen	
Connections	Verbindung mit einem bestimmten Domänencontroller herstellen
Help	Zeigt diese Hilfeinformation an.
List current selections	Listet den aktuellen Standort, Server, Namenskontext sowie die aktuelle Domäne auf
List domains	Listet alle Domänen auf, die Querverweise haben
List domains in site	Listet die Domänen im gewählten Standort auf
List naming contexts	Führt die bekannten Namenskontexte auf
List roles for connected server	Listet die Funktionen auf, die dem verbundenen Server bekannt sind
List servers for domain in site	Listet die Server für die gewählte Domäne und den Standort auf.

List servers in site	Listet die Server im gewählten Standort auf
List sites	Listet die Standorte im Unternehmen auf
Quit	Zum vorherigen Menü wechseln
Select domain %d	Domäne %d zur gewählten Domäne machen
Select naming context %d	Namenskontext %d zum gewählten Namenskontext machen
Select server %d	Server %d zum gewählten Server machen
Select site %d	Standort %d zum gewählten Standort machen

8. Geben Sie `List Sites` ein. Die Ausgabe könnte etwa so aussehen:

```
select operation target: list sites

4 Standort(e) gefunden
0 - CN=Frankfurt,CN=Sites,CN=Configuration,DC=firma,DC=de
1 - CN=Hamburg,CN=Sites,CN=Configuration,DC=firma,DC=de
2 - CN=Bonn,CN=Sites,CN=Configuration,DC=firma,DC=de
3 - CN=Wiesbaden,CN=Sites,CN=Configuration,DC=firma,DC=de
```

9. Geben Sie `select site <#>` ein, wobei `<#>` die Nummer des Standorts ist, der den zu entfernenden Server enthält.

```
select operation target: select site 1

Standort - CN=Hamburg,CN=Sites,CN=Configuration,DC=firma,DC=de
Keine aktuelle Domäne
Kein aktueller Server
Kein aktueller Namenskontext
```

10. Geben Sie `list domains in site` ein. Die Beispielausgabe sieht so aus:

```
select operation target: list domains in site

1 Domäne(n) gefunden
0 - DC=firma,DC=de
```

11. Geben Sie `Select Domain <#>` ein, wobei `<#>` die Nummer der Domäne ist, die den zu entfernenden Server enthält.

```
select operation target: select domain 0


Standort - CN=Hamburg,CN=Sites,CN=Configuration,DC=firma,DC=de
Domain - DC=firma,DC=de
Kein aktueller Server
Kein aktueller Namenskontext
```

12. Geben Sie `list servers for domain in site` ein. Die Beispielausgabe sieht wie folgt aus:

```
select operation target: list servers for domain in site

2 Server gefunden
0 - CN=SRV01,CN=Servers,CN=Hamburg,CN=Sites,CN=Configuration,
➥ DC=firma,DC=de
0 - CN=SRV02,CN=Servers,CN=Hamburg,CN=Sites,CN=Configuration,
➥ DC=firma,DC=de
```

13. Geben Sie `Select Server <#>` ein, wobei `<#>` die Nummer des zu entfernenden Servers ist.

```
select operation target: select server 0

Standort - CN=Hamburg,CN=Sites,CN=Configuration,DC=firma,DC=de
➥ Domäne- DC=firma,DC=de
Server - CN=SRV02,CN=Servers,CN=Hamburg,CN=Sites,CN=Configura
➥ tion,DC=firma,DC=de
DSA-Objekt - CN=NTDS Settings,CN=SRV02,CN=Servers,CN=Hamburg
➥,CN=Sites,
     CN=Configuration,DC=firma,DC=de
Computerobjekt - CN=SRV02,OU=Domain Controllers,DC=firma,DC=de
```

14. Jetzt haben wir das zu löschende Serverobjekt ins Visier genommen. Geben Sie `q` ein, um wieder zum Prompt `metadata cleanup:` zu gelangen.

15. Geben Sie `remove selected server` ein. Ein Fenster mit der Bitte um Bestätigung des Vorgangs wird angezeigt.

16. Klicken Sie auf `JA` – nun ist es vollbracht. Die Beispielausgabe sieht so aus:

```
Metadata cleanup: remove selected server

"CN=SRV02,CN=Servers,CN=Hamburg,CN=Sites,CN=Configuration,DC=
➥ firma,DC=de"
        von Server "srv01.firma.de" entfernt.
```

17. Verlassen Sie `Ntdsutil` und warten Sie, bis die Änderung repliziert ist.

Mit der selben Vorgehensweise können Sie eine Domäne zu entfernen, die nicht vollständig gelöscht ist, als der letzte Domänencontroller außer Dienst gestellt wurde. Seien Sie aber vorsichtig, damit Sie keine intakten Domänen zu löschen.

2.3.5 Ausfall eines FSMO

Es gibt ein paar Dinge, bei denen der Multimasterbetrieb nicht benutzt werden kann; diese müssen vielmehr von einem einzigen Server erledigt werden. Diese Aufgaben werden als FSMOs (Flexible Single Master Operations) bezeichnet; die Server, denen die Aufgaben zugewiesen sind, als FSMO-Rollenmaster.

- Domänen-Naming-Master. Dieser FSMO ist für die Eindeutigkeit von Domänennamen in einem Forest verantwortlich. Es gibt einen Domänen-Naming-Master pro Forest.
- Schemamaster. Dieser FMSO besitzt die einzige Schreib-/Lesekopie des Schemas. Es gibt einen Schemamaster pro Forest.
- PDC-Emulator. Dieser FSMO repliziert die Aktualisierungen auf die Windows NT-BDCs in Mixed. Er dient ferner als Berufungsinstanz für Passwörter und als Zeitstandard. Es gibt einen PDC-Emulator pro Domäne.
- RID-Master. Dieser FSMO speichert RID-Hauptliste. In Mixed werden diese RIDs der Reihenfolge nach ausgegeben. In Native bekommt jeder Domänencontroller einen Pool von RIDs vom RID-Master. Es gibt normalerweise einen RID-Master pro Domäne.
- Infrastrukturmaster. Dieser FMSO ist für die schnelle Übermittlung von Namensänderungen zuständig, die domänenübergreifende Gruppenmitgliedschaften im Forest betreffen. Es gibt einen Infrastrukturmaster pro Domäne.

Ein kurzer Ausfall eines FSMO-Rollenmasters erfordert keine speziellen Schritte, aber wenn ein Rollenmaster für längere Zeit vom Netz geht, sollten Sie seine Rolle bzw. Rollen auf einen anderen DC übertragen.

Fällt ein FSMO-Rollenmaster vollständig aus und kann nicht mehr eingesetzt werden, dann müssen Sie ihm die Rollen entziehen und sie einem anderen DC übergeben. Bei einer Übertragung muss der vorherige Rollenmaster online sein, um die Transferanfrage annehmen zu können. Beim Entzug ist der vorherige Rollenmaster nicht online, und der neue Rollenmaster nimmt sich einfach die Rolle.

Nach dem Entzug einer Rolle dürfen Sie den alten Rollenmaster nie wieder ans Netz bringen. Nur so verhindern Sie, dass der alte Rollenmaster ungültige Informationen ausgibt oder eine alternative Möglichkeit für das Update kontrollierter Strukturen wie des Schemas darstellt.

Festlegung eines Rollenmasters

Was einen bestimmten Server zu einem Flexible-Single-Master-Operations-Rollenmaster macht, ist ein Attribut in dem Active-Directory-Objekt, das eine bestimmte FSMO kontrolliert. Beispielsweise kontrolliert das Domänen-Objekt die PDC-Emulator-Rolle. Ein FSMO-Attribut in diesem Objekt bedeutet, dass der definierte Name des Servers als PDC-Emulator festgelegt wurde. Wenn Sie eine Rolle übergeben oder entziehen, verändern Sie den definierten Namen, der diesem Rollenmaster-Attribut zugewiesen ist.

Einen verlorenen PDC-Emulator wiederherstellen

Die einzige Ausnahme, in der man alte Rollenmaster wieder in Betrieb nehmen darf, bildet der PDC-Emulator. Wenn man einen früheren PDC-Emulator wieder online nimmt, erfährt er via Replikation den Namen des neuen PDC-Emulators und stellt anstandslos all seine Rollenmaster-Aktivitäten ein.

Allerdings liegt in der Praxis der RID-Master normalerweise auf demselben Server wie der PDC-Emulator, sodass Sie den Server doch nicht wieder einsetzen können. Wenn Sie einen ehemaligen RID-Master wieder einsetzen, kann es passieren, dass zwei Objekte dieselbe RID erhalten, was die Sicherheit und Datenbankkonsistenz gefährden würde. Wenn sich RID-Master und PDC-Emulator auf demselben Server befinden und ihm diese Rollen entzogen und einem anderen Server übertragen wurden, dann formatieren Sie die Platten des ursprünglichen Servers und installieren das Betriebssystem neu.

Übertragung eines FSMO-Rollenmasters

Für den Transfer eine FSMO auf einen neuen Rollenmaster können Sie wahlweise eine MMC-Konsole oder ein Befehlszeilenutility verwenden. Die Auswahl der Konsole hängt von der zu übertragenden Rolle ab. Die Tabelle zeigt eine Liste der FSMO-Rollen und der benötigten MMC-Konsolen samt Sicherheitshinweisen.

Informationen zur Übertragung von FSMO-Rollenmastern

FSMO-Rolle	Konsole	Hinweise
PDC-Emulator	Active Directory-Benutzer und -Computer	Der PDC-Emulator muss mit allen alten BDCs in Kontakt bleiben. Da der PDC-Emulator auch als „Berufungsinstanz" für die Passwort-Validierung dient, muss er mit dem WAN verbunden bleiben.
RID-Master	Active Directory-Benutzer und -Computer	Dieser Rollenmaster sollte auf demselben Server wie der PDC-Emulator liegen. Falls Sie den RID-Master unbedingt auf einen anderen Domänencontroller legen wollen, dann achten Sie auf eine sehr gute Anbindung an den PDC-Emulator. In Mixed muss der RID-Master für die Erzeugung von neuen Benutzern, Computern und Gruppen verfügbar sein.
Infrastrukturmaster	Active Directory-Benutzer und -Computer	Legen Sie diesen Rollenmaster auf einem beliebigen Server ab, der kein GC-Server ist. Achten Sie auch auf den Hinweis „Betrieb des Infrastrukturmasters".

Domänen-Naming-Master	Active Directory-Domänen und -Vertrauensstellungen	Halten Sie diesen Rollenmaster und den Schemamaster auf einem DC. Diese beiden Rollen sind in Forest einzigartig, weswegen die WAN-Verbindung zuverlässig sein muss.
Schemamaster	Schema-Snap-In	Siehe oben

Betrieb des Infrastrukturmasters

Wenn Sie einen Sicherheitsprincipal (Benutzer, Gruppe oder Computer) in eine Gruppe aufnehmen, dann wird der DN des Sicherheitsprincipals einem Attribut namens Members des Gruppenobjekts in Active Directory hinzugefügt. Active Directory erhält die interne Konsistenz, indem es einen Back-Link auf das Objekt erzeugt, das den Sicherheitsprincipal repräsentiert. So kann das Member-Attribut aktualisiert werden, wenn sich der Objektname ändert.

Setzen Sie nun als Administrator einer Domäne in einem Forest einen Sicherheitsprincipal aus einer anderen Domäne in eine Gruppe Ihrer Domäne, steht Active Directory vor einem Dilemma. Es kann keinen Back-Link auf ein Objekt in einem anderen Domänen-Namenskontext erzeugen.

Es löst dieses Problem, indem es ein Phantomobjekt erzeugt, was nichts weiter als eine Struktur in seinem Domänen-Namenskontext ist, die aus dem DN des Objekts, seinem GUID und seiner SID besteht. Der Infrastrukturmaster in einer Domäne entdeckt Namensänderungen an Sicherheitsprincipals, die von Phantomeinträgen in seiner eigenen Domäne repräsentiert werden. Ohne diesen Dienst würden die Namen, die bei Gruppenmitgliedschaftslisten angezeigt werden, nicht den evtl. geänderten Namen in den Quelldomänen entsprechen. Das betrifft nicht den Zugang zu Ressouren, weil die SID nicht verändert wurde.

Der Infrastrukturmaster erledigt diese Aufgabe, indem er regelmäßig die Liste der Phantomeinträge durchgeht und die Namen gegen die Namen im GC prüft. Falls er einen Unterschied feststellt, aktualisiert er den Phantomeintrag so, dass er den neuen Namen repräsentiert. Diese Veränderung wird dann an die anderen DCs in der Domäne repliziert, die eine Kopie des Phantomeintrags besitzen.

GC-Server verfügen bereits über eine Kopie der Objekte von anderen Domänen und speichern deswegen keine Phantomeinträge. Deswegen dürfen Sie den Infrastrukturmaster keinem GC-Server zuweisen.

Ändern eines Rollenmasters über eine MMC-Konsole

1. Öffnen Sie die Konsole, die Sie für die Übertragung des FSMO benötigen.

2. Wenn Sie sich nicht beim DC befinden, der der neue Rollenmaster werden soll, gehen Sie folgendermaßen vor: Klicken Sie mit der rechten Maustaste auf das

oberste Symbol im Verzeichnisbaum (das denselben Namen wie die Konsole hat) und wählen Sie aus dem Kontextmenü den Eintrag VERBINDUNG MIT DOMÄNENCONTROLLER HERSTELLEN.

3. Wählen Sie den Namen des DC aus, der neuer Rollenmaster sein soll. Dadurch wird die Anforderung seitens LDAP erfüllt, die Bindung an den Server herzustellen, damit Sie sich authentifizieren können.

4. Klicken Sie auf OK, um sich mit dem Domänencontroller zu verbinden.

5. Klicken Sie mit der rechten Maustaste auf das oberste Symbol (Domänen und Vertrauensstellungen, Schema) bzw. die Domäne (Benutzer und Computer) und wählen Sie diesmal BETRIEBSMASTER aus dem Kontextmenü. Das Fenster BETRIEBSMASTER wird angezeigt.

6. Wählen Sie die Registerkarte, die der zu übertragenden Rolle zugeordnet ist.

7. Überprüfen Sie, ob der angezeigte DC dem Server entspricht, auf den Sie die Rolle übertragen wollen.

8. Klicken Sie auf ÄNDERN. Sie werden nun zur Bestätigung aufgefordert.

9. Klicken Sie auf OK. Nach kurzer Zeit werden Sie darüber informiert, dass der Betriebsmaster erfolgreich übertragen wurde. Auf der Registerkarte BETRIEBSMASTER erscheint der neue Name nun unter BETRIEBSMASTER.

10. Klicken Sie auf OK, um das Fenster zu schließen.

Jetzt müssen Sie warten, bis die Replikation volle Konvergenz erreicht hat, damit alle Domänencontroller über den neuen Rollenmaster Bescheid wissen.

Sie können die Konsole ACTIVE DIRECTORY-STANDORTE UND -DIENSTE oder den Replikationsmonitor Replmon aus den Support-Tools verwenden, um die Replikation zu erzwingen.

Ändern eines Rollenmasters über Ntdsutil

Mögen Sie grafische Tools nicht (oder verwalten Sie Ihre Server mit Telnet oder SSH), dann können Sie auch das Utility Ntdsutil zur Übertragung von Rollenmastern zwischen DCs verwenden. Sowohl ursprünglicher als auch künftiger Rollenmaster müssen online sein. Gehen Sie wie folgt vor:

1. Melden Sie sich anschließend über ein Benutzerkonto mit Administratorrechten an der Domäne an. Bezieht sich die Rollenänderung auf den Schema- oder Domänen-Naming-Master, dann benötigen Sie die Administratorrechte auch für den Konfigurationsnamenskontext.

2. Starten Sie `Ntdsutil`.

3. Geben Sie `roles` an der Eingabeaufforderung `ntdsutil:` ein. Dadurch wird die Eingabeaufforderung `FSMO maintenance:` geöffnet.

4. Geben Sie `?` ein. Die Optionsliste wird angezeigt.

Ntdsutil-Befehle	
?	Zeigt diese Hilfeinformationen an
Connections	Verbindung mit einem bestimmten Domänencontroller herstellen
Help	Zeigt diese Hilfeinformationen an
Quit	Zeigt diese Hilfeinformationen an
Seize domain naming master	Funktion der Domäne auf dem verbundenen Server überschreiben
Seize infrastructure master	Funktion der Infrastruktur auf dem verbundenen Server überschreiben
Seize PDC	Funktion des primären Domänencontrollers auf dem verbundenen Server überschreiben
Seize RID master	Funktion des primären Domänencontrollers auf dem verbundenen Server überschreiben
Seize schema master	Funktion des Schemas auf dem verbundenen Server überschreiben
Select operation target	Standorte, Server, Domänen, Funktionen und Namenskontexte wählen
Transfer domain naming master	Den verbundenen Server zum Domain Naming Master machen
Transfer infrastructure master	Den verbundenen Server zum Infrastrukturmaster machen
Transfer PDC	Server zum primären Domänencontroller machen
Transfer RID master	Server zum RID-Master machen
Transfer schema master	Den verbundenen Server zum Schemamaster machen

5. Geben Sie `connections` ein. Die Eingabeaufforderung `server connections` wird angezeigt.

6. Geben Sie `?` ein. Die Optionsliste wird angezeigt.

Ntdsutil-Befehle	
?	Zeigt diese Hilfeinformationen an
Clear creds	Frühere Verbindungsinformationen löschen
Connect to domain %s	Verbindung mit DNS-Domänennamen herstellen

Connect to server %s	Verbindung mit Server, DNS-Namen oder IP-Adresse herstellen
Help	Zeigt diese Hilfeinformationen an
Info	Verbindungsinformationen anzeigen
Quit	Zum vorherigen Menü wechseln
Set creds %s %s %s	Verbindungsinformationen als Domäne, Benutzer und Kennwort festlegen. Verwenden Sie „NULL" für ein Null-Kennwort, * um das Kennwort an der Konsole einzugeben.

7. Geben Sie `Connect to Server %s` ein, wobei `%s` der vollqualifizierte DNS-Name des DCs ist, auf den Sie die Rolle übertragen wollen. Geben Sie beispielsweise `Connect to Server srv01.firma.de` ein. Falls erfolgreich, erhalten Sie den folgenden Statusbericht:

```
server connections: connect to server srv01.firma.de.

Bindung mit "srv01.firma.de" ...
Eine Verbindung mit "srv01.firma.de" unter Verwendung der Benutzerinformationen des lokal angemeldeten Benutzers wurde hergestellt.
```

8. Wenn Sie ein anderes Konto verwenden wollen, benutzen Sie den Befehl `Set Creds` vor der Eingabe des Befehls `Connect to Server`.

9. Geben Sie `q` ein, um das Modul zu verlassen und wieder zur Eingabeaufforderung `FSMO Maintenance` zu wechseln.

10. Wählen Sie eine zu übertragende Rolle und geben Sie das entsprechende Kommando. Wollen Sie etwa den PDC-Emulator übertragen, geben Sie den Befehl `Transfer PDC` ein.

11. Es erscheint ein Fenster, in dem Sie den Vorgang bestätigen müssen. Klicken Sie auf OK, um den Rollentransfer zu starten.

12. Falls die Übertragungsvorgang nicht funktioniert, erhalten Sie eine Fehlermeldung, und die Rolle verbleibt beim ursprünglichen Master. Wäre etwa der Zielserver bereits Rollenmaster, wird Ihnen dies mitgeteilt. Klappt die Übertragung, zeigt Ntdsutil eine aktuelle Rollenmasterliste nach Ausführung des Vorgangs an.

Einen Rollenmaster entziehen

Wenn ein Domänencontroller, der einen FSMO-Rollenmaster hostet, komplett ausfällt, lassen sich die Rollen nicht mit den MMC-Konsolen übertragen – Sie müssen sie mithilfe von `Ntdsutil` entziehen. Zur Erinnerung: Wenn Sie einem Rollenmaster seine Rolle entziehen, darf dieser nie wieder online gehen. Das heißt im Klartext: Festplatte formatieren und neu installieren.

Stellen Sie sicher, dass der Domain Controller, der als neuer Rollenmaster vorgesehen ist, online ist, und gehen Sie wie folgt vor:

1. Melden Sie sich über ein Konto mit Administratorrechten an der Domäne an. Bezieht sich die Rollenänderung auf den Schema- oder Domänen-Naming-Master, benötigen Sie auch Administratorrechte für den Konfigurationsnamenskontext.

2. Starten Sie `Ntdsutil`.

3. Geben Sie `Roles` an der Eingabeaufforderung `Ntdsutil` ein. Dadurch wird die Eingabeaufforderung `FSMO Maintenance:` geöffnet.

4. Geben Sie `Connections` ein. Die Eingabeaufforderung `Server Connections` wird angezeigt.

5. Geben Sie `Connect to Server`, gefolgt vom vollqualifizierten DNS-Namen des DC, auf den Sie die Rolle übertragen wollen, ein. Falls erfolgreich, erhalten Sie den folgenden Statusbericht:

```
server connections: connect to server srv01.firma.de.

Bindung mit "srv02.firma.de" ...
Eine Verbindung mit "srv01.firma.de" unter Verwendung der Benutzerinformationen des lokal angemeldeten Benutzers wurde (sic!) hergestellt.
```

6. Geben Sie `q` ein, um das Modul zu verlassen und wieder zur Eingabeaufforderung `FSMO Maintenance` zu wechseln.

7. Wählen Sie eine zu übertragende Rolle. In diesem Beispiel soll der RID-Master übertragen werden. Geben Sie etwa `Seize RID Master` ein. Es erscheint ein Fenster, in dem Sie den Vorgang bestätigen müssen. Klicken Sie auf OK, um den Rollentransfer zu starten. (Falls der derzeitige Rollenmaster online ist, nimmt `Ntdsutil` einfach eine normale Übertragung vor.)

8. Falls der Übertragungsvorgang nicht funktioniert, erhalten Sie eine Fehlermeldung und die Rolle verbleibt beim ursprünglichen Master. Verläuft die Übertragung problemlos, dann zeigt Ntdsutil eine aktuelle Rollenmasterliste.

2.3.6 Verlust zentraler Replikationskomponenten

Wenn ein Domänencontroller ausfällt, dann merken seine Replikationspartner, dass er nicht mehr auf Update-Anfragen antwortet. Die Partner benachrichtigen den KCC-Dienst, der sich an die Arbeit macht und Verbindungsobjekte erzeugt, die den ausgefallenen Domain Controller umgehen, ganz wie die gelben Umleitungsschilder bei Straßensperrungen.

Wird der ausgefallene Domänencontroller wieder verfügbar, merken dies seine Replikationspartner und informieren ihren KCC-Dienst. Der KCC stellt die Verbindungsobjekte zum Domänencontroller wieder her und entfernt die Umleitung.

Das kann ein Weilchen dauern, verlieren Sie also nicht die Geduld. Sie sollten zum Schluss einen Eintrag im Ereignisprotokoll sehen, dass der KCC die Verbindungsobjekte erstellen und der DRA die Namenskontexte synchronisieren konnte.

Die Situation wird etwas komplizierter, wenn der ausgefallene Domänencontroller spezielle Inter-Site-Replikationsaufgaben hatte. Damit sind Brückenkopfserver und ISTGs gemeint.

Neuen bevorzugten Brückenkopfserver auswählen

Die Replikation zwischen Sites erfolgt über ausgewählte Domänencontroller, die Brückenköpfe heißen. Normalerweise kümmert sich der KCC selbst um den Ausfall eines Brückenkopfservers, ohne dass Sie als Administrator eingreifen müssten. Er sortiert die vorhandenen Domänencontroller nach ihrer GUID und nimmt dann den Server mit der höchsten GUID.

Sie könnten aber vorziehen, dass der KCC die Brückenköpfe aus einer bestimmten Gruppe von Servern auswählt. Beispielsweise sollte nach Möglichkeit ein GC-Server als Brückenkopf dienen, damit partielle Namenskontexte ohne Zwischenstation zum nächsten Standort repliziert werden. Deswegen lohnt es sich, die Kandidatenliste auf GC-Server zu beschränken. Um einen Domänencontroller als bevorzugten Brückenkopfserver auszuweisen, verwenden Sie die Servereigenschaften in `ACTIVE DIRECTORY-STANDORTE UND -DIENSTE` (siehe Bild 2).

Bild 2: Eigenschaften eines Servers in Active Directory-Standorte und -Dienste, der als bevorzugter Brückenkopf für IP-Kommunikation ausgewählt ist.

Weisen Sie stets mindestens zwei bevorzugte Brückenkopfserver aus. Wenn Sie nur einen auswählen und dieser dann ausfällt, unterbricht die Replikation, bis Sie einen neuen wählen. Wenn der letzte verfügbare Brückenkopfserver ausfällt, müssen Sie so schnell wie möglich einen neuen bevorzugten Brückenkopfserver festlegen, damit die Replikation wieder anfangen kann.

ISTG auswählen

Der Ausfall eines ISTG stellt kein unmittelbares Problem dar. Die einzig echte Aufgabe des ISTG ist die Erstellung von Verbindungen zwischen Brückenkopfservern. Das geschieht nicht sehr häufig, was aber nicht heißen soll, dass Sie einen Ausfall ignorieren dürfen. ISTG informiert seine Replikationspartner über seine Präsenz, indem er ein Attribut in seinem Objekt alle 30 Minuten aktualisiert. Wenn eine Stunde ohne Update verstreicht, merkt der KCC auf den anderen Domänencontrollern des Standorts, dass ISTG nicht mehr verfügbar ist, und sie suchen sich aus ihrer Mitte einen neuen aus. ISTG kann mit dem Eigenschaftenfenster des Objekts `NTDS SITE SETTINGS in ACTIVE DIRECTORY-STANDORTE UND -DIENSTE` (Bild 3) identifiziert werden.

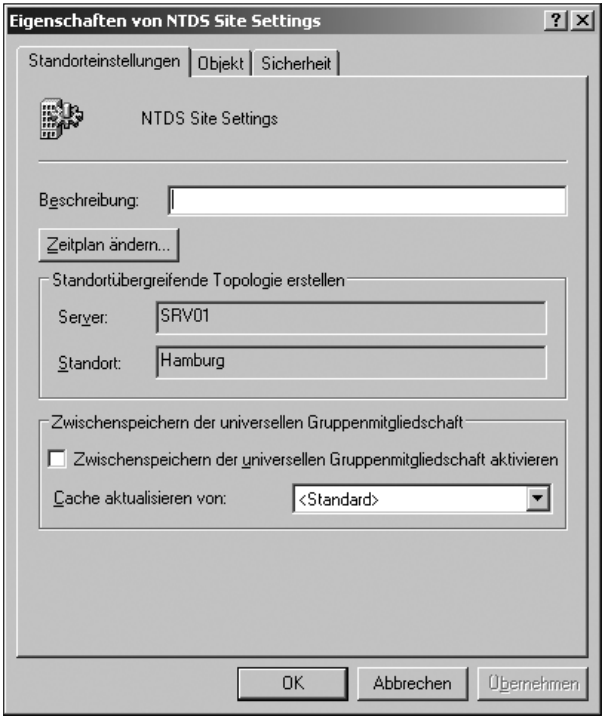


Bild 3: Eigenschaften von NTDS Site Settings mit dem ISTG-Server des Standorts.

Der KCC verwendet für die Wahl des neuen ISTG denselben Algorithmus wie für die Wahl eines neuen Brückenkopfs. Er nimmt den Domänencontroller mit der höchsten GUID am Standort. Im Fall von ISTG gibt es aber keine Möglichkeit, einen bevorzugten Domänencontroller auszuweisen.

Repliken mit Dsastat prüfen

Wenn die Replikation erst einmal läuft, kann es nicht schaden, wenn Sie sich davon überzeugen, dass die Repliken auf den verschiedenen Domänencontrollern identisch sind. Am einfachsten geht das mit dem Utility `Dsastat`, das Teil der Support-Tools ist. Öffnen Sie eine Kommandozeile und geben Sie `dsastat -loglevel:info` ein. Je nach Geschwindigkeit der Anbindungen zu den Replikationspartnern kann es fünf bis 15 Minuten dauern, bis das Utility fertig ist. Am Ende erhalten Sie eine Liste aller Objekte in den Repliken samt deren Größen, sodass Sie Zahl und Größe der Objekte vergleichen können.

Ausfall einer WAN-Leitung

Wenn eine WAN-Leitung zusammenbricht, merken die Brückenköpfe auf beiden Seiten, dass sie keine Replikation mehr vom Partner ziehen können. Wenn eine alternative Verbindung (mit höheren Kosten) zum anderen Standort existiert, verwendet der DRA-Agent auf den Brückenköpfen diese Verbindung automatisch. Der DRA informiert auch den ISTG, der dann versucht, neue Verbindungen zu den anderen Brückenköpfen herzustellen.

Sie sollten sich nicht in den Betrieb von DRA und ISTG einmischen. Wenn es ihnen nicht gelingt, einen brauchbaren Replikationspfad zu finden, dann müssen Sie ohne Replikation leben, bis die Leitung wieder funktioniert.

2.3.7 Sicherung von Active Directory

In der guten alten Zeit konnte man in einer kleinen NT-Domäne die gesamte Registry auf eine einzige Notfalldiskette kopieren oder aber mit `Rdisk -S` auf die Festplatte, wenn der SAM zu groß für eine Diskette war. Lang ist's her. Heute existiert das Tool `Rdisk` nicht einmal mehr.

Active Directory-Operationen benötigen die Registry und zahlreiche andere Systemdateien, sodass Sie weite Teile des Systemverzeichnisses sichern und wiederherstellen müssen. Microsoft bezeichnet diese Dateien als Systemstatus. Bild 4 zeigt die Liste der Systemstatus-Dateien, wie sie in Ntbackup angezeigt werden. Zu ihnen gehören:

- alle vom Windows-Dateischutzsystem geschützten Dateien (entwpricht so gut wie allen Dateien in `C:\Windows`)
- die Systemdateien `Ntdetect.com`, `Ntldr` und `Bootsect.dat`
- die Active Directory-Datenbank `Ntds.dit` samt der zugehörigen Protokoll- und Kontrollpunktdateien

- bestimmte zum Internet Explorer gehörende und gemeinsam genutzte Dateien aus dem Verzeichnis `Programme`
- alle Registry-Zweige aus dem Verzeichnis `\Windows\System32\Config` (aktualisierte Kopien landen in `\Windows\Repair`)
- die COM+-Klassenregistrierdatenbank
- der Inhalt des Verzeichnisses `\SYSVOL`
- die Zertifikatsdienstdateien (falls installiert)
- die Clusterdienstdateien (falls installiert)

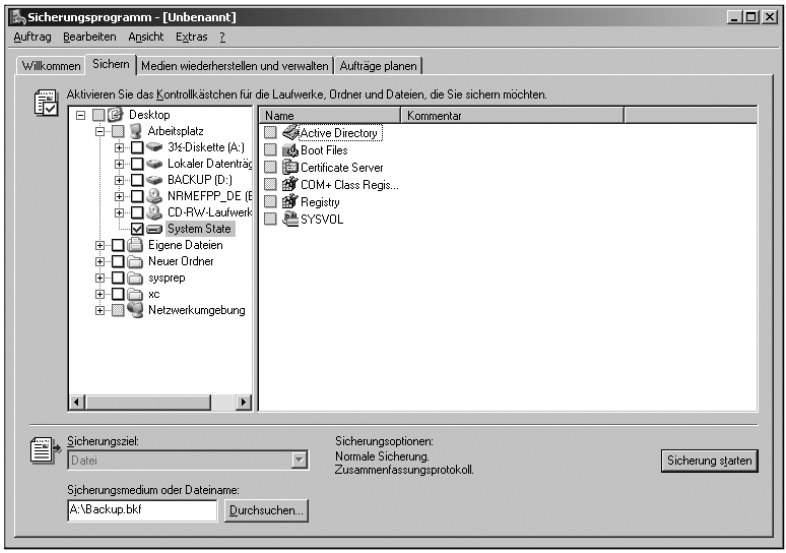


Bild 4: Ntbackup mit den Dateien des Systemstatus.

Diese Sicherungsstrategie erhält zwar die Konsistenz zwischen den verschiedenen Datenspeichern. Wenn Sie aber auch nur einen kleinen Fehler machen (der jedoch einen nicht wiederherstellbaren Teil der Registry betrifft), dann müssen Sie möglicherweise alle Systemstatusdateien wiederherstellen – einschließlich des Verzeichnisses! Hier wird beschrieben, wie Sie die Systemstatus-Dateien mit `Ntbackup` sichern und wieder einspielen können. `Ntbackup` ist eine funktionsmäßig beschränkte Version von `Veritas Backup Exec`. Fremdanbieter haben Backup-Produkte im Portfolio, die dieselben Funktionen bieten. Dazu gehört die Vollversion von Backup Exec, Computer Associates ArcServe, Legato Networker, Tivoli Storage Manager, BEI Corporation UltraBac, CommVault Galaxy u.a. Alle diese Hersteller bieten 2003-kompatible Utilitys an. Achten Sie auf die Version, denn ein Windows 2000-Backup-Utility könnte nicht voll kompatibel zu Server 2003 sein.

Warum Active Directory-Backups unerlässlich sind

Möglicherweise fragen Sie sich, wozu AD-Backups notwendig sind. Schließlich sollten Sie in jeder Domäne mindestens drei Domänencontroller betreiben, die jeweils über eine Komplettkopie von Active Directory verfügen. Wenn einer dieser Server ausfällt oder sogar zwei kaputtgehen, so bleibt Ihnen immer noch der Dritte als Ersatz. Sie können schnell einen anderen Windows-Mitgliedsserver zum Domänencontroller befördern und die Fehlertoleranz wieder herstellen.

Die nahe liegendste Antwort zu „warum Active-Directory-Backups unerlässlich sind" lautet, dass Mr. Murphy es merkt, wenn Sie keine Backups machen, und dann das Universum so manipuliert, dass Sie Ihre drei Domänencontroller gleichzeitig verlieren. Ein Feuer könnte Ihren Serverraum komplett zerstören, und dann müssten Sie Active Directory an einem entfernten Standort wiederherstellen. Sie sollten niemals ohne volles Backup leben, damit sich die Sterne niemals in einer Konstellation einfinden, die nicht Ihren Interessen entspricht.

Doch die wahrscheinlichere Katastrophenvariante ist ein Fehler auf Seiten des Administrators; das wird früher oder später jedem einmal passieren. Sie sind müde oder abgelenkt, löschen oder ändern das falsche Objekt und schon entwickelt sich die ganze Angelegenheit zur Katastrophe. Wenn Sie versehentlich eine ganze OU mit mehreren tausend Benutzern, Computern und Gruppenobjekten löschen, werden die anderen Domänencontroller davon umgehend per Replikation informiert. Sie bekommen diese OU nur noch von Band zurück.

Sie müssen nicht all ihre Domänencontroller sichern. Suchen Sie sich zwei oder drei in Ihrer Domäne aus und sichern Sie den Systemstatus dieser Rechner. Lassen Sie auf Domänencontrollern keine Applikationen laufen, die es erfordern würden, dass sie von lokalen Administratoren gesichert werden.

Systemstatus-Backup durchführen

Ein Systemstatus-Backup wird stets im laufenden Betrieb durchgeführt, d.h. der Rechner hängt am Netz und verrichtet seinen normalen Dienst. Der PnP-Manager sollte Ihr Bandlaufwerk erkennen und die passenden Treiber installieren. Unter Umständen müssen Sie den Wechselmedien-Manager verwenden, um mit Ihren Medienpools zu jonglieren. Gehen Sie zur Sicherung des Systemstatus mit `Ntbackup` wie folgt vor:

1. Legen Sie ein frisches Band in das Bandlaufwerk.

2. Starten Sie `Ntbackup` über START/ALLE PROGRAMME/ZUBEHÖR/SYSTEMPROGRAMME/SICHERUNG. Das Fenster SICHERUNG öffnet sich.

3. Klicken Sie auf `ERWEITERTEN MODUS`, um den Assistenten loszuwerden.

4. Wählen Sie den Reiter SICHERN.

5. Erweitern Sie ggf. die Ansicht, bis die Option SYSTEM STATE angezeigt wird. Es ist dies die letzte Option unter den Laufwerkbuchstaben.

6. Aktivieren Sie die Option SYSTEM STATE.

7. Wählen Sie unter SICHERUNGSZIEL das entsprechende Bandlaufwerk, das Sie für die Sicherung verwenden.

8. Wenn Sie in eine Datei sichern wollen, wählen Sie DATEI und geben dann unter SICHERUNGSMEDIUM ODER DATEINAME den Dateipfad und -namen ein. Stellen Sie sicher, dass die Dateien auf zuverlässigen Wechselmedien oder auf einem Netzlaufwerk gespeichert werden, das für eine mögliche Datenwiederherstellung sicher zur Verfügung steht. Sichern Sie nicht auf die lokale Festplatte.

9. Wählen Sie aus dem Menü EXTRAS den Eintrag OPTIONEN. Das Fenster OPTIONEN öffnet sich.

10. Wählen Sie den Reiter SICHERUNGSART.

11. Wählen Sie unter STANDARDSICHERUNGSART die Option KOPIEREN. So verhindern Sie, dass das System das Archivbit zurücksetzt. Das stellt sicher, dass die Systemstatusdateien auch beim allnächtlichen Backup mitkopiert werden.

12. Wählen Sie nun den Reiter SICHERUNGSPROTOKOLL.

13. Markieren Sie den Radiobutton DETAILS. Dadurch werden viele Informationen einschließlich der Namen aller gesicherten Dateien protokolliert. Normalerweise würden dies zu viele Informationen sein, um damit vernünftig arbeiten zu können, aber Sie sollten die Option zumindest einmal wählen, um eine Liste der Dateien zu erhalten, die bei der Systemstatussicherung gesichert werden.

14. Klicken Sie auf OK, um die Änderungen zu speichern und wieder zum Hauptfenster zurückzukehren.

15. Diese Sicherung soll nicht irgendwann, sondern sofort ablaufen. Klicken Sie also auf SICHERUNG STARTEN.

16. Ist dies das erste Mal, dass Sie dieses Band verwenden, dann kann eine Fehlermeldung angezeigt werden, laut der keine unbenutzten Medien des gewählten Typs, jedoch unerkannte Medien verfügbar sind. Sie können auch aufgefordert werden, das Überschreiben vorhandener Daten zu bestätigen, falls das Band erkannt wird. Wenn Sie sicher sind, dass Sie kein Band mit wichtigen Daten eingelegt haben, klicken Sie auf OK. Verschiedene Bandsysteme können unterschiedliche Formatierungs- und Abrufschemata haben, weswegen die angezeigten Meldungen variieren können. In Ihrer Systemdokumentation finden Sie genauere Hinweise. Ntbackup verwendet das MTF-Format (Microsoft Tape Format).

17. Erkennt das System das Band bzw. – bei Verwendung von Wechselmedien – den Dateiablageort, dann beginnt das Backup. Das Fenster STATUS: SICHERUNGSVORGANG wird geöffnet.

18. Wenn die Sicherung abgeschlossen ist, wird ein letztes Fenster mit Statistiken angezeigt. Gegebenfalls steht im Statusfeld steht, dass Dateien übersprungen wurden. Klicken Sie auf BERICHT, um dass Sicherungsprotokoll anzeigen zu lassen. Oft ist finden Sie hier `DO_NOT_REMOVE_NtFrs_Preinstall_Directory` im SYSVOL-Verzeichnis. Dort befinden sich Dateien, die während der Migration in die FRS-Datenbank hierher kopiert wurden und übersprungen werden können.

Gehen Sie die Dateiliste im Protokoll durch. Sie werden feststellen, dass die Verzeichnisdateien selbst im Protokoll nicht auftauchen, aber keine Sorge, sie sind trotzdem gesichert. Sie sehen das an dem einen Eintrag, der angibt, dass Active Directory gesichert wurde.

Auch die Registry-Dateien sind gesichert, allerdings in Form eines speziellen Ordners namens `\Registry` und nicht unter ihrem tatsächlichen Standort, `\Windows\System32\Config`. Dieser Ordner `\Registry` ist ein flüchtiger temporärer Ordner, in dem ein Schnappschuss der Registry zu Sicherungszwecken abgelegt wird. Dadurch wird die Sperrung der Registry-Dateien vermieden, die den Zugriff auf die Registry während der Sicherung unterbrechen würde.

Active Directory wiederherstellen

Es gibt zwei Grundszenarien, die eine Wiederherstellung der Active-Directory-Datenbank nötig machen:

- der Komplettausfall eines Domänencontrollers, sodass die Daten vollständig vom Band wieder eingespielt werden müssen
- ein Fehler eines Administrators, der den partiellen oder gesamten Verlust von Active Directory zur Folge hat

Im ersten Szenario erfolgt die Bandwiederherstellung der Systemstatusdateien (zu denen Active Directory gehört) in Verbindung mit einer Wiederherstellung des Betriebssystems. Wenn der frisch wiederhergestellte Domänencontroller wieder online geht, aktualisieren ihn seine Replikationspartner mit den Änderungen, die es seit der Erstellung des Backups gab. Deswegen können Sie auch von einem älteren Band wiederherstellen, falls es Probleme mit dem Band von letzter Nacht gibt.

DSRM-Passwort

Wenn Sie Active Directory bei einem Domänencontroller wiederherstellen, müssen Sie sich bei diesem Server mit dem Administratorkonto im lokalen SAM anmelden. Vielleicht kennen Sie aber das Passwort nicht.

Deswegen hat Microsoft ein neues Feature in das Utility `Ntdsutil` eingebaut, mit dem das lokale Administratorpasswort geändert werden kann. Dieses Feature heißt `Reset DSRM (Directory Services Restore Mode) Administrator Passwort`. Mit Administratorrechten auf einem Domänencontroller können Sie dieses Feature verwenden, um das Administratorkonto im SAM des Domänencontrollers zu ändern.

Autoritative Wiederherstellung

Eine Standard-Systemstatus-Wiederherstellung holt Objekte zurück, die aus Active Directory gelöscht wurden. Wenn der frisch wiederhergestellte Domänencontroller nun von seinen Partnern repliziert, werden die wiederhergestellten Objekte umgehend wieder in den `Deleted Objects`-Container verschoben, und die ganze Arbeit war umsonst.

Wenn Sie einen Teil von Active Directory wiederherstellen müssen (ein einzelnes Objekt oder eine versehentlich gelöschte OU) oder auch (im Falle einer irreparablen Beschädigung) die ganze Datenbank, so müssen Sie dafür sorgen, dass die Objekte und ihre Eigenschaften auf dem Band auf die anderen Domänencontroller repliziert werden. Genau das leistet eine `autoritative Wiederherstellung`.

Eine autoritative Wiederherstellung ist eigentlich gar keine Wiederherstellung. Sie wird nach der eigentlichen Bandwiederherstellung durchgeführt und markiert die Objekte, die in den Repliken auf den anderen Domänencontrollern überschrieben werden sollen. Das geschieht, indem 100.000 zu den PVNs der einzelnen Eigenschaften der autoritativ wiederhergestellten Objekte addiert wird.

Im Folgenden finden Sie ein Repadmin-Beispiellisting, das zeigt, wie ein Benutzerobjekt vor und nach einer autoritativen Wiederherstellung aussieht. Das Attribut `ObjectClass` wird bei der autoritativen Wiederherstellung nicht angerührt, da es ein speziell für die Indizierung benötigtes Objekt ist.

Lassen Sie größte Vorsicht walten, wenn Sie eine autoritative Wiederherstellung des Konfigurations-Namenskontexts oder der ganzen Active Directory-Datenbank durchführen. Tun Sie dies ja nicht, wenn Ihnen auch nur im Entferntesten unklar sein könnte, was die Konsequenzen des Überschreibens von Systemkonfigurationsparametern sein könnten. Das gilt ganz besonders, wenn Sie Exchange 2000 oder andere Active Directory-abhängige Applikationen laufen haben. Sie brauchen nicht die ganze Datenbank wiederherzustellen, um nur eine OU zurückzukriegen. Seien Sie ruhig wählerisch.

Wer darf Active Directory wiederherstellen?

Wenn Sie eine verteilte IT-Organisation mit Administratoren auf der ganzen Welt haben, könnte sich Ihnen die Frage stellen, wer eine Verzeichnis-Wiederherstellung durchführen kann. Es sollte klar sein, dass nur qualifizierte Leute Bandwiederherstellungen auf Domänencontrollern durchführen dürfen. Und Sie sollten auch wissen, ob Sie ein Problem beseitigen können, ohne die zentrale IT-Abteilung jenseits des Atlantiks anzurufen.

Die Durchführung einer Systemstatus-Wiederherstellung (was auch die Active Directory-Datenbank umfasst) erfordert das lokale Administratorpasswort im SAM auf dem Domänencontroller. Dieses Passwort heißt Directory Service Recovery Password. Wenn Sie dieses Passwort kennen, dann können Sie eine autoritative Wiederherstellung eines Teils oder der ganzen AD-Datenbank vornehmen, und zwar unabhängig davon, ob Sie nun Rechte über einen bestimmten Teil des Verzeichnisses haben oder nicht. Schließlich läuft ja der Active Directory-Dienst nicht, während Sie die autoritative Wiederherstellung durchführen, und so hat das System keine Chance, Ihre Anmeldedaten abzufragen und zu validieren.

Sie sollten das lokale Administratorpasswort von Domänencontrollern scharf bewachen und es oft austauschen. Andererseits kann jeder, der physikalischen Zugriff auf einen Domänercontroller hat, dort mit einem Utility wie ERD-Commander das lokale Administratorpasswort festlegen und vollen Zugriff erhalten.

Unternehmen Sie Folgendes, um Ihre AD-Datenbank zu schützen:

- Geben Sie nur den zuverlässigsten Administratoren das Recht, den Systemstatus auf Domänencontrollern wiederherzustellen.
- Sichern Sie den Systemstatus nur auf wenigen, ausgewählten Domänencontrollern. Die Administratoren, die diese Backups durchführen, sollten zu den zuverlässigsten Leuten der Firma gehören.
- Verhindern Sie den physikalischen Zugriff auf Domänencontroller an entfernten Standorten. Setzen Sie Server ohne Disketten- und CD-Laufwerk ein.

Zeitlimit für Backupbänder

Das passiert jeder IT-Abteilung irgendwann. Sie wollen ein Band einspielen und merken, dass die Bänder von letzter Nacht entweder nicht lesbar sind oder das Backup nicht durchgeführt wurde. Sie gehen zur Bibliothek und stellen fest, dass manche Bänder so alt sind, dass Sie die Sonne durch die Oxidschicht sehen können. Und ein paar der brauchbaren Bänder klemmten im Laufwerk, und es wurde überhaupt nichts auf sie geschrieben. Irgendwann finden Sie ein benutzbares Band, aber das ist dann schon ein bis zwei Wochen alt. Und Sie fragen sich, ob Sie wirklich Active Directory von diesem Band wiederherstellen können.

Die gute Nachricht ist, dass Sie den Systemstatus von einem etwas älteren Band einspielen können, ohne Active Directory zu gefährden. Sobald die Systemstatus-Wiederherstellung abgeschlossen ist und Sie den Domänencontroller neu starten, erhält die wiederhergestellte Kopie von Active Directory Updates von den Replikationspartnern und wird uptodate gebracht. Wenn Sie dagegen eine autoritative Wiederherstellung durchführen, verlieren Sie alle zwischenzeitlichen Änderungen wie geänderte Passwörter, Veränderungen an Gruppenmitgliedschaften, neue Domänentrusts usw. Sie müssen also sehr vorsichtig damit sein, ein älteres Band für eine autoritative Wiederherstellung zu verwenden.

Tombstone-Lebensdauer

Es gibt zwei Grenzen, die der Verwendung einer älteren Kopie von Active Directory gesetzt sind. Die erste Grenze ist die Tombstone-Lebensdauer von gelöschten AD-Objekten. Wenn ein AD-Objekt gelöscht wird, erlebt es zunächst so eine Art Fegefeuer. Das Objekt wird all seiner Attribute (mit wenigen Ausnahmen) entkleidet und in die Tiefen des `Containers Deleted Objects` geschleudert, in dem es 60 Tage lang sitzt und fault. Am Ende der 60 Tage – der voreingestellten Tombstone-Lebensdauer – wird das Objekt vom Garbage-Collection-Prozess endgültig aus der Datenbank entfernt.

Das bedeutet, dass Sie auf keinen Fall den Systemstatus (und damit Active Directory) von einem Band installieren dürfen, das älter als 60 Tage ist. Lassen Sie sich das Risiko anhand eines Beispiels erklären.

Angenommen, Sie löschen ein Objekt aus AD und führen dann eine Systemstatus-Wiederherstellung mit dem Band von letzter Nacht durch. Wenn Sie kein autoritatives Backup durchführen, wird das Objekt sofort wieder gelöscht, sobald der Do-

mänencontroller Updates von seinen Replikationspartnern zieht. Das Update sagt: „Dieses Objekt ist bei mir im Container `Deleted Objects`. Verschiebe auch du deine Kopie des Objekts in den Container Delected Objects."

Doch wenn Sie von einem Band wiederherstellen, das älter als 60 Tage ist, dann werden die Replikationspartner den Tombstone aus dem Deleted Objects-Container entfernt haben. In diesem Fall gibt es keine Möglichkeit mehr, mit der der frisch wiederhergestellte Domänencontroller angewiesen werden könnte, das alte Objekt zu löschen. Die frisch wiederhergestellten Objekte werden zu Untoten. Sie sind aus allen Repliken des Namenskontexts gelöscht, außer der des wiederhergestellten Computers. Mit anderen Worten: Die Active Directory-Datenbank ist nicht mehr konsistent.

Vergessen Sie niemals diese 60-Tage-Frist. Hüten Sie sich vor Wiederherstellungsplänen, die eine ältere Kopie des Active Directory in Ihr System einspielen könnten. Machen Sie etwa keine Images von Domänencontrollern für Katastrophenfälle. Die CD mit dem Image wird am Tag 61 von Ihrem besten Freund zu Ihrem schlimmsten Albtraum. Wenn Sie Images in Ihre Wiederherstellungsstrategie integrieren wollen, dann machen Sie das Image vor der Hochstufung des Servers zum Domänencontroller. Stellen Sie das Image wieder her und stufen Sie dann den Rechner zum Domänencontroller hoch. Das repliziert eine frische Kopie des Verzeichnisses von einem anderen Domänencontroller.

Wenn Sie alle Kopien von Active Directory bei einer Katastrophe verlieren, dann bleibt Ihnen nichts anderes übrig, als das neueste Band einzuspielen und dann alle Änderungen durchzuführen, die es in der Zwischenzeit gegeben hatte, wie Passwortänderungen oder Änderungen von Gruppenmitgliedschaften.

Wiederherstellungen von Active Directory und Vertrauensstellungen

Es gibt noch ein zweites Limit für Systemstatus-Wiederherstellungen von älteren Bändern. Externe Vertrauensstellungen zu anderen Forests oder NT-Domänen verwenden Passwörter, die sich alle 7 Tage ändern. Wenn ein neues Passwort ausgehandelt wird, wird das alte Passwort nicht einfach vergessen, sondern gespeichert. Werden jedoch die Passwörter von einem Band wiederhergestellt, das älter als 14 Tage ist, dann müssen Sie die externen Trusts überprüfen und eine Neuverhandlung des Passworts erzwingen. Schlimmstenfalls müssen Sie den Trust entfernen und neu einrichten.

Autoritative Wiederherstellung und Sysvol

FRS (File Replication Service) repliziert den Inhalt von `Sysvol` bei allen Domänencontrollern der Domäne. Wenn Sie die GPC-Objekte in Active Directory autoritativ wiederherstellen, ohne `Sysvol` in den Zustand zurückzuführen, in dem es zum Zeitpunkt des Systemstatus-Backups war, dann riskieren Sie eine Differenz zwischen den GPC-Objekten in AD und den GPT-Dateien in Sysvol.

Es gibt keine autoritative Wiederherstellung von `Sysvol`. Stattdessen müssen Sie eine Kopie der Systemstatus-Dateien inklusive der `Sysvol`-Dateien an eine ande-

re Stelle wiederherstellen und dann die Sysvol-Dateien herüberkopieren, nachdem Sie nach einer autoritativen Wiederherstellung von AD neu starten. Dies wird folgendermaßen durchgeführt:

1. Führen Sie eine normale Systemstatus-Wiederherstellung an den Original-Ort durch. Booten Sie nicht neu!

2. Führen Sie eine zweite Systemstatus-Wiederherstellung an einen anderen Ort durch. Dies schützt die älteren Sysvol-Dateien, damit Sie diese nach dem Neustart verwenden können.

3. Führen Sie eine autoritative Wiederherstellung der AD-Objekte oder -Container durch, die Sie zurückhaben wollen. Darunter sollten sich Objekte befinden, die mit Gruppenrichtlinien zu tun haben – denn sonst sind Sie in der falschen Schrittfolge gelandet und haben gar keinen Grund, sich wegen Sysvol Sorgen zu machen.

4. Lassen Sie den Domänencontroller neu booten und sehen Sie zu, dass der Sysvol-Inhalt von den Replikationspartnern aktualisiert wird. Das ist sehr wichtig. Sie dürfen erst dann weitermachen, wenn beim Inhalt von Sysvol auf allen Domänencontrollern volle Konvergenz erreicht ist.

5. Kopieren Sie nun auf dem Domänencontroller, auf dem Sie die autoritative Wiederherstellung durchführten, den Inhalt von Sysvol von dem alternativen Ort in das Standard-Sysvol. Damit überschreiben Sie die vorhandenen Dateien. Sie können auch die Ordner Policies und Scripts löschen und sie vom Alternativort herüberkopieren, wenn Sie alle GPT-Dateien entfernen wollen.

6. Warten Sie wiederum, bis beim Inhalt von Sysvol Konvergenz bei den Domänencontrollern erreicht ist.

7. Prüfen Sie nach, ob die Clients die richtigen Gruppenrichtlinien erhalten.

Einen Systemstatus wieder einspielen

Wenn Sie den Systemstatus wieder einspielen, überschreiben Sie die vorhandenen Dateien auf dem Rechner. Viele der Systemstatus-Dateien sind Datenbanken, die im laufenden Betrieb des Servers gewöhnlich gesperrt sind. Das gilt für die Active Directory-Datenbank, die Registry-Zweige, die Zertifikatdatenbank und andere.

Sie müssen also für die Systemstatus-Wiederherstellung den Rechner in eine Konfiguration booten, in der diese Datenbanken nicht laufen. Dies ist der Verzeichnisdienst-Wiederherstellungs-Modus (Directory Service Restore Mode, DSRM) eine der Optionen des abgesicherten Modus von Windows. Drücken Sie beim Standard-Bootmenü auf (F8) und wählen Sie dann diese Option aus dem Menü. Falls Sie kein Bootmenü sehen, drücken Sie unmittelbar nach dem POST auf (F8). Damit ist die gedrückte Taste im Tastaturpuffer und wird erkannt, sobald Ntldr startet. Der DSRM lädt die Netzwerktreiber, sodass Sie eine Bandwiederherstellung über das Netzwerk vornehmen können; er aktiviert aber weder Active Directory noch sonst irgendeine andere kritische Datenbank. Dieser Modus setzt die Umgebungsvariable SAFEBOOT_OPTION auf DSREPAIR. Diese Variable muss gesetzt sein, denn sonst führt Ntdsutil keine autoritative Wiederherstellung durch.

Da im DSRM Active Directory nicht verfügbar ist, müssen Sie das Passwort des Administratorkontos im lokalen SAM eingeben. Das ist das Passwort, das Sie eingaben, als der Server zum Domänencontroller befördert wurde.

Das DSRM-Passwort ändern

Wenn Sie das DSRM-Passwort vergessen oder einen Server übernommen haben, bei dem Sie nicht wissen, was bei `Dcpromo` als Passwort eingegeben wurde, so können Sie das Passwort mit einem Utility von SysInternals (www.sysinternals.com) namens `ERD Commander` ändern. Es gibt zwei Versionen dieses Utilitys. Die kostenlose Version kann das Administratorpasswort nicht ändern, die kostenpflichtige dagegen schon. Sie könnten solche Passwörter auf einem Zettel notieren, den Sie dann im Servergehäuse einschließen. Auch ein Ausdruck der Datenträgerverwaltung wäre nützlich; vielleicht braucht später ein anderer Administrator das ursprüngliche Partitionslayout, um einen Festplattenfehler zu beheben.

Wenn Sie sich im abgesicherten Modus befinden, führen Sie die Systemstatus-Wiederherstellung wie folgt durch:

1. Starten Sie auf dem Domänencontroller, auf dem Sie Active Directory wiederherstellen wollen, das System im DSRM.

2. Legen Sie das Backupband mit den Systemstatus-Dateien ein.

3. Öffnen Sie das `AUSFÜHREN`-Fenster und geben Sie `Ntbackup` ein.

4. Wählen Sie den Reiter `MEDIEN WIEDERHERSTELLEN UND VERWALTEN`.

5. Erweitern Sie den Baum, bis Sie das Laufwerk und eine Liste früherer Jobs sehen. Wenn Sie den Baum beim Band-Symbol erweitern, müssen Sie u.U. warten, bis das Band zurückgespult ist. Wenn Sie einen Katalog auf Festplatte haben, wird das System die Signatur im Katalog mit der Signatur auf dem Band vergleichen. Haben Sie keinen Katalog auf Festplatte, müssen Sie das Band katalogisieren. Klicken Sie das Medium mit der rechten Maustaste an und wählen Sie `KATALOG`.

6. In dem Baum, den der Bandkatalog anzeigt, setzen Sie `SYSTEM STATE`.

7. Klicken Sie auf `WIEDERHERSTELLUNG STARTEN`. Eine Meldung weist Sie darauf hin, dass die Systemstatusdateien stets die vorhandenen Dateien überschreiben, wenn Sie nicht an einen Alternativort wiederherstellen wollen. Sie sollten nicht an Alternativorte wiederherstellen, weil fürs manuelle Kopien zu viele Dateien und zu viele Variablen involviert wären. Halten Sie den Atem an und lassen Sie das System überschreiben.

8. Klicken Sie auf `JA`, um die Meldung zu bestätigen. Das Bandlaufwerk arbeitet.

9. Nachdem die Wiederherstellung vollzogen wurde, klicken Sie auf `BERICHT` und sehen sich das Protokoll an, um sicherzugehen, dass alle Dateien fehlerfrei wiederhergestellt wurden.

10. Schließen Sie den Editor und das Wiederherstellungsfenster. Ihnen wird ein Neustart angeboten. Lehnen Sie das ab. Klicken Sie auf `NEIN` und beenden Sie anschließend das Backup-Programm.

Die Systemstatus-Wiederherstellung ist nun vollzogen. Wenn Sie nicht einzelne Objekte oder Container wiederherstellen wollen, können Sie den Domänencontroller neu starten und die Veränderungen seit dem Backup replizieren lassen. Wenn Sie einzelne Komponenten des Verzeichnisses wiederherstellen wollen, lesen Sie den nächsten Abschnitt.

Eine autoritative Verzeichniswiederherstellung durchführen

Da autoritative wiederhergestellte Eigenschaften höhere PVNs als die Repliken auf anderen Domänencontrollern haben, werden die Eigenschaften nach außen repliziert und überschreiben andere Repliken. Deswegen kann eine autoritative Wiederherstellung eine Menge Replikationstraffic nach sich ziehen.

Planen Sie mehrere Stunden ein und legen Sie ein besonderes Augenmerk auf Domänencontroller am anderen Ende einer langsamen WAN-Leitung. Wenn Sie bereit sind, folgen Sie der nächsten Schrittfolge:

1. Öffnen Sie eine Befehlszeile.

2. Sarten Sie `Ntdsutil`.

3. Geben Sie an der Eingabeaufforderung ntdsutil: den Befehl `authoritative restore` ein, um die gleichnamige Eingabeaufforderung aufzurufen:

Ntdsutil-Befehle	
?	Zeigt diese Hilfeinformationen an
Help	Zeigt diese Hilfeinformationen an
List NC CRs	Listet Partitionen und Querverweise. Sie benötigen die Querverweise einer Anwendungsverzeichnispartition, um sie wiederherzustellen
Quit	Zum vorherigen Menü wechseln
Restore database	Autorisierende Wiederherstellung der gesamten Datenbank
Restore database verinc %d	... und Überschreiben der Versionserhöhung
Restore object %s	Autorisierende Wiederherstellung eines Objekts
Restore object %s verinc %d	... und Überschreiben der Versionserhöhung
Restore subtree %s	Autorisierende Wiederherstellung einer untergeordneten Struktur
Restore subtree %s verinc %d	... und Überschreiben der Versionserhöhung

4. Wählen Sie eine Option entsprechend Ihrem Anliegen. Sie müssen den DN kennen. Angenommen, Sie wollen ein einzelnes Objekt wiederherstellen, dann könnten Sie beispielsweise Folgendes eingeben: `restore object cn=fberger,ou=Berlin,dc=Firma,dc=de`.

5. Ein Fenster mit der Bitte um Bestätigung wird angezeigt. Klicken Sie auf JA, um die autoritative Wiederherstellung zu starten. Die Beispielausgabe sieht wie folgt aus:

```
Die DIT-Datenbank wird geöffnet... Der Vorgang ist abge-
schlossen.
Aktuelle Zeit 05-05-03 03:59:37.
Die letzte Datenbankaktualisierung erfolgte 05-05-03
14:27.52.
Die Versionsnummern des Attributs werden um 100000 erhöht.
Die zu aktualisierenden Datensätze werden gezählt...
Gefundene Einträge: 0000000001
Der Vorgang ist abgeschlossen.
1 Einträge wurden für die Aktualisierung gefunden.
Datensätze werden aktualisiert...
Verbleibende Datensätze: 0000000000
Der Vorgang ist abgeschlossen.
1 Datensätze wurden einwandfrei aktualisiert.
Die autorisierende Wiederherstellung wurde einwandfrei abge-
schlossen.
```

Wird die Wiederherstellung nicht einwandfrei abgeschlossen, dann könnte die Datenbank beschädigt sein. Probieren Sie eine sanfte Wiederherstellung und eine harte Reparatur (s.u.). Versuchen Sie dann eine weitere autoritative Wiederherstellung. Klappt es dann immer noch nicht, dann stellen Sie die Daten von Band wieder her. Versuchen Sie es dann auf einem anderen Domänencontroller. Und dann können Sie langsam den Microsoft-Support anrufen.

6. Verlassen Sie nun Ntdsutil und starten Sie den Domänencontroller neu. Sobald er wieder am Netz ist, erzwingen Sie die Replikation manuell.

2.3.8 Verzeichnis pflegen

Active Directory sollte man soviel Aufmerksamkeit schenken wie jeder anderen Datenbank. Manchmal treten in der Datenbank Lücken auf, dann ist eine Defragmentierung nötig. Manchmal gerät sie durcheinander, dann muss neu indiziert werden. Manchmal wird sie beschädigt und muss dann repariert werden. Und manchmal wird sie eben auch komplett zerschossen und muss dann wiederhergestellt werden. Das Tool für diese Aufgaben ist Ntdsutil (NT Directory Service Utility).

Für manche Dinge verwendet Ntdsutil feste Befehlsabfolgen für ein anderes Utility namens Esentutl, dem Enkel des für Exchange entwickelten Datenbankhilfsprogramms Eseutil. Esentutl kennt eine große Anzahl von Schaltern für das Festlegen und Steuern von Wiederherstellungsaufgaben und Integritätschecks. Ntdsutil bietet diese Optionen in einem Menü. Die beiden meistgebrauchten Optionen sind:

- Komprimierung und Neuindizierung des Verzeichnisses
- Reparieren der Verzeichnisdatenbank

Active Directory-Datenbank defragmentieren

Wenn Sie je länger mit Exchange 5.5 gearbeitet haben, dann wissen Sie, wie zerbrechlich die alte ESE-Datenbank sein kann. Die neue und verbesserte ESENT-Engine benötigt nicht dermaßen viel Aufmerksamkeit. Alle 12 Stunden läuft die Garbage Collection durch und entfernt Objekte, die seit mehr als 60 Tagen getombstoned sind. Dann defragmentiert der Garbage Collector die Datenbank. Es gibt also keinen Grund für Offline-Defragmentierungen oder Reindizierungen.

Wenn Sie eine Offline-Defragmentierung mit `Ntdsutil` durchführen, dann komprimiert das Utility die Datenbank, indem es den Inhalt der vorhandenen `Ntds.dit` in eine neue Datei desselben Namens kopiert, die in einem von Ihnen benannten Temporärverzeichnis abgelegt wird. Ist die Komprimierung abgeschlossen, dann überschreiben Sie einfach mit der neuen Datei die alte, oder Sie lassen das System auf die neue Datei verweisen. Die Protokolldateien sind nicht mehr gültig und können ignoriert werden.

Der einzige Grund für eine Offline-Defragmentierung ist, dass Sie Festplattenspeicher zurückhaben wollen, den `Ntds.dit` einnimmt. Die Online-Defragmentierung packt zwar die Datenbank, gibt aber keinen Festplattenspeicher frei. Folgendermaßen können Sie eine Offline-Defragmentierung durchführen:

1. Fahren Sie den Domänencontroller im Verzeichnisdienst-Wiederherstellungsmodus hoch und starten Sie Ntdsutil.

2. Geben Sie an der Eingabeaufforderung `Ntdsutil`: den Befehl `Files` ein, um die Eingabeaufforderung `File Maintenance` zu öffnen.

3. Geben Sie `Compact to <verzeichnis>` ein, wobei `<verzeichnis>` der Name des Temporärverzeichnisses ist, in dem die komprimierte NTDS.DIT gespeichert wird. Die Beispielausgabe:

```
file maintenance: compact to C:\xxx
Die Datenbank [Current] wird geöffnet.
Folgendes Verzeichnis wird erstellt: C:\xxx
Befehl wird ausgeführt: C:\WINDOWS\system32\esentutl.exe /
d"C:\WINDOWS\NTDS\ntds
.dit" /t"C:\xxx\ntds.dit" /p /o
Initiating DEFRAGMENTATION mode...
            Database: C:\WINDOWS\NTDS\ntds.dit
      Temp. Database: C:\xxx\ntds.dit
                  Defragmentation Status (% complete)
       0    10   20   30   40   50   60   70   80   90  100
       |----|----|----|----|----|----|----|----|----|----|
Note:
It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the
state   it was in at the time of that backup.
Operation completed successfully in 9.304 seconds.
Erstellter Prozessbeendigungscode 0x0(0)
```

Wenn die Komprimierung einwandfrei durchgeführt wurde, tun Sie Folgendes:

```
copy "C:\xxx\ntds.dit" "C:\WINDOWS\NTDS\ntds.dit"
```

und die alten Protokolldateien löschen:

```
del C:\WINDOWS\NTDS\*.log
```

4. Kopieren Sie nun die neue `Ntds.dit` in das ursprüngliche Verzeichnis `\NTDS`. Wenn Sie wollen, können Sie das neue Verzeichnis auch lassen, wo es ist, und die Verzeichniszeiger anpassen:

```
Set Path Backup <verzeichnis>
Set path DB <verzeichnis>
Set path logs <verzeichnis>
Set path working dir <verzeichnis>
```

Wenn Ihre Protokolle auf einem anderen Laufwerk liegen, lassen Sie den Befehl `Set path logs` an dieser Stelle weg.

Active Directory-Datenbank reparieren

Wenn die ESE-Engine auf ein Problem trifft, das aufgrund beschädigter Datenbankseiten, einer beschädigten Indexdatei oder einer Kombination aus beiden auftritt, dann müssen Sie die Datenbank reparieren. Symptome für derartige Probleme sind enstprechende Einträge im Ereignisprotokoll, Konsolenfehler oder Neustarts mit Fehlermeldungen vom LSASS (Local Security Authority Subsystem). Active Directory kennt zwei Reparaturphasen:

- `Sanfte Wiederherstellung`. Diese Phase restauriert die Einträge anhand von Protokoll- und Prüfpunktdateien, gefolgt von den Indizes.
- `Harte Reparatur`. Diese Phase geht prinzipiell genauso vor, löscht aber zusätzlich alle beschädigten Seiten. Dadurch können Daten verloren gehen, weswegen Sie keine harte Reparatur vornehmen sollten, sofern es noch andere Alternativen gibt. Vor einer Wiederherstellung der Datenbank sollten Sie immer eine Sicherungskopie anfertigen. Bei Server 2003 ist die harte Reparatur nicht mehr über `Ntdsutil` zugänglich. Wenn Sie unbedingt wollen, können Sie direkt `Esentutl` verwenden.

Gehen Sie für eine sanfte Wiederherstellung wie folgt vor:

1. Öffnen Sie eine Befehlszeile.

2. Starten Sie `Ntdsutil`.

3. Geben Sie an der Eingabeaufforderung `Ntdsutil:` den Befehl `Files` ein, um die Eingabeaufforderung `File Maintenance` zu öffnen.

4. Geben Sie Recover ein. Die Beispielausgabe:

```
file maintenance: recover
Befehl wird ausgeführt: C:\WINDOWS\system32\esentutl.exe /
redb /l"C:\WINDOWS\NTD
S" /s"C:\WINDOWS\NTDS" /8 /o
Initiating RECOVERY mode...
Logfile base name: edb
Log files: C:\WINDOWS\NTDS
System files: C:\WINDOWS\NTDS
Performing soft recovery...
Operation completed successfully in 2.243 seconds.
Erstellter Prozessbeendigungscode 0x0(0)
Es wird empfohlen, eine semantische Datenbankanalyse durch-
zuführen, wenn die Wiederherstellung einwandfrei abgeschlos-
sen wurde. Dadurch wird die semantische Konsistenz gewähr-
leistet.
```

In der Regel geht dieser Vorgang relativ schmerzlos über die Bühne. Wenn jedoch Probleme auftreten, versucht das System, sie zu lösen. Sie sollten von Ntdsutil aus eine semantische Datenbankanalyse durchführen, um die internen Namenverweise in der Datenbank zu prüfen und ggf. zu reparieren. Sollte die sanfte Wiederherstellung jedoch nicht zum Ziel führen, dann müssen Sie die harte Reparatur wählen. Zuvor könnten und sollten Sie allerdings noch den Support bei Microsoft kontaktieren – die haben vielleicht ein paar weniger radikale Vorschläge. Normalerweise gibt es wenig Gründe, überhaupt eine harte Reparatur durchzuführen. Doch wenn Sie unbedingt wollen, gehen Sie wie folgt vor:

1. Geben Sie an der Eingabeaufforderung den Befehl `esentutl /p c:\windows\ntds\ntds.dit /o` ein. Falls sich Ihre AD-Datenbank an anderer Stelle befindet, müssen Sie natürlich den Pfad entsprechend ändern. Die Beispielausgabe sieht so aus:

```
C:\Dokumente und Einstellungen\Administrator>esentutl /p c:\
➥ windows\ntds\ntds.dit /o

Initiating REPAIR mode...
Database: c:\windows\ntds\ntds.dit
Temp. Database: TEMPREPAIR3180.EDB
Checking database integrity.
Scanning Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
..................................................
Integrity check successful.

Note:
t is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
repair, the database will be rolled back to the state it was
in at the time of that backup.
Operation completed successfully in 5.718 seconds.
```

2. Nehmen Sie wie bereits weiter oben beschrieben eine vollständige Sicherung der Systemstatusdateien vor.

Active-Directory-Hilfsdateien verschieben

Wenn Sie einen Domänencontroller hochstufen, können Sie festlegen, wo die Haupt-AD-Datei `Ntds.dit` und die Protokolldateien abgelegt werden. Sie können diesen Ort ändern, wenn Sie der Meinung sind, dass Sie die Performance steigern könnten, wenn Sie die Protokolle auf ein anderes Array legen oder die Dateien von der Systempartition nehmen.

Um diese Dateien zu verschieben, müssen Sie in den Verzeichnisdienst-Wiederherstellungsmodus booten. Dafür müssen Sie das lokale Administratorpasswort kennen. Sie sollten die Dateien stets auf einer NTFS-Partition ablegen, um von der höheren Sicherheit und guten Random-Access-Performance zu profitieren. Wenn Sie die Dateien verschieben wollen, verwenden Sie diese Schrittfolge:

1. Booten Sie in den AD-Wiederherstellungsmodus.

2. Öffnen Sie eine Befehlszeile.

3. Geben Sie `Ntdsutil` ein.

4. Geben Sie `files` ein, um zum Prompt `file maintenance:` zu kommen. Mit `?` erhalten Sie eine Befehlsübersicht:

Ntdsutil-Befehle	
?	Zeigt diese Hilfeinformationen an
Checksum	Physische Jet-Integritätsprüfung durchführen
Compact to %s	Datenbank in das angegebene Verzeichnis komprimieren
Header	Jet-Datenbankheader speichern
Help	Zeigt diese Hilfeinformationen an
Info	Informationen zu den DS-Dateien zurückgeben
Integrity	Logische Jet-Integritätsprüfung durchführen
Move DB to %s	Datenbank zum angegebenen Verzeichnis verschieben
Move logs to %s	Protokolldateien zum angegebenen Verzeichnis verschieben
Quit	Zum vorherigen Menü wechseln
Recover	Durchführen einer Datenbankwiederherstellung
Set default folder security	Sicherheitseinstellungen von NTDS-Ordnern auf Standardwerte zurücksetzen

Set path backup %s	Verzeichnispfad der Onlinesicherung festlegen
Set path DB %s	Pfad zur Datenbankdatei festlegen
Set path logs %s	Verzeichnispfad für die Protokollierung festlegen
Set path working dir %s	Pfad für das Arbeitsverzeichnis von NTDS festlegen

5. Verwenden Sie `move db to %s` oder `move logs to %s`, um die Datenbank oder die Protokolle zu verschieben. Ersetzen Sie %s mit einem vollständigen Pfad, wie `D:\Windows\NTDS`. (mha)

Weiterführende Infos

Dieser Artikel basiert auf Kapitel Zehn des Standardwerks „Windows Server 2003 für Insider“ von William Boswell aus dem Verlag Markt + Technik. Sie können dieses über 1300 Seiten starke Buch auch in unserem tecCHANNEL-Buchshop unter dem Webcode „buchshop“ bestellen oder als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Katastrophenszenarien bei Active Directory	434994	S.117
Active-Directory-Verwaltung in Windows 2003	402153	–
Windows Server Automaten	434408	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

3. Sicherheit

In vielen Netzen findet sich eine bunte Mischung aus Windows und verschiedenen Unix- und Linux-Derivaten als Server und Client. Dennoch sollen alle Server von möglichst allen Arbeitsstationen aus erreichbar sein. Zum Glück gibt es mit dem Samba-Projekt eine Möglichkeit, Windows-Clients mit Linux-Servern zu verbinden. Welche Stolperfallen es dabei zu vermeiden gilt, zeigt der erste Artikel dieses Kapitels. Im zweiten Artikel gehen wir darauf ein, wie Sie einen Linux-Rechner unabhängig von der verwendeten Distribution absichern und vor Gefahren durch Hacker und böswillige Mitarbeiter schützen.

3.1 Zugriffskontrolle bei Samba und *nix

Fortgeschrittene Windows-Benutzer sind häufig verwirrt, wenn sich eine Änderung der Besitzrechte an Dateien oder Verzeichnissen auf dem Samba-Server nicht so auswirkt, wie sie es erwarten. MS-Administratoren verwirrt es oft, wenn sie versuchen, Ihre Daten mit Zugriffskontroll-Listen vor unerlaubten Zugriffen zu schützen.Viele UNIX-Administratoren sind nicht mit der MS Windows-Umgebung vertraut. Besondere Probleme ergeben sich aus den Benutzerwünschen bezüglich der Kontrolle von Dateien und Verzeichnissen und deren Einrichtung.

Das Problem rührt aus den Unterschieden bei den Datei- und Verzeichnis-Benutzerrechten der beiden Systeme her. Diesen Unterschied kann auch Samba nicht wirklich aus der Welt schaffen, aber es schafft eine Brücke zwischen den Umgebungen. Die POSIX-(UNIX, LINUX-)Zugriffskontroll-Technologie (ACLs) gibt es schon seit Jahren, aber sie wurde nie sehr intensiv genutzt.

Dies erklärt vielleicht auch, warum es so lange gedauert hat, bis die die ACL-Technik in kommerzielle Linux-Produkte eingebunden wurde. MS-Administratoren wird dies erstaunen, da diese Technik seit Jahren elementarer Bestandteil von Windows-Produkten ist.

Dieses Kapitel soll die Punkte im Einzelnen klären, die mit Samba-3 nötig und möglich sind, damit Administratoren eine optimale Zugriffsverwaltung für ihre Windows-Benutzer einrichten können. Samba ist nicht primär dafür gedacht, eine Unix-Plattform in eine Windows-Plattform zu verwandeln, sondern soll die bestmögliche Kompatibilität zwischen den beiden Systemen schaffen.

3.1.1 Möglichkeiten und Vorteile

Samba bietet dem Administrator eine sehr große Flexibilität beim Zugriff auf die verschiedenen Ressourcen. Hier sind es die Zugriffskontrollmöglichkeiten der aktuellen Version 3 von Samba.

Unix-Datei- und -Verzeichnis-Berechtigungen

Samba arbeitet mit den UNIX-Dateizugriffskontrollen zusammen. Benutzer greifen dabei als Windows-Benutzer auf Samba zu. Informationen über den Benutzer werden beim Einloggen übergeben. Samba benutzt diese Login-Informationen, um zu entscheiden, ob einem Benutzer Zugriff auf Systemdaten gewährt werden soll oder nicht. Dieses Kapitel enthält eine Übersicht über UNIX-Berechtigungen für Nutzer, die diese nicht kennen oder diese für etwas verwirrend halten.

Samba-Netzlaufwerksdefinitionen

Beim Konfigurieren von Netzlaufwerken mit Samba in der Datei smb.conf kann der Administrator Berechtigungen des darunter liegenden Dateisystems verändern und beeinflussen. Dies ermöglicht teilweise eine Annäherung an das Verhalten, das Windows-Benutzer erwarten. Dieser Weg ist aber nur selten die beste Lösung. Die grundlegenden Möglichkeiten werden hier beschrieben.

Samba-Netzlaufwerkskontroll-Listen

Wie in Windows NT ist es auch in Samba möglich, Netzlaufwerkskontroll-Listen zu erstellen. Einige Anwender machen Gebrauch davon. Es ist zurzeit eine der leichtesten Möglichkeiten, Zugriffskontrolle zu erreichen, im Gegensatz zu anderen komplexeren Methoden.

MS Windows-Zugriffskontroll-Listen und UNIX-Zugriffskontroll-Listen

Der Gebrauch von UNIX-Kontroll-Listen ist nur möglich, wenn diese Funktionen in dem darunter liegenden Dateisystem implementiert sind. In jedem anderen Fall ist deren Nutzung nicht möglich. Aktuelle Unix-Systeme sollten diese Unterstützung bieten. Es gibt Patches für den Linux-Kernel, die diese Möglichkeit implementieren, falls sie noch nicht vorhanden ist. Viele Unix-Systeme werden mit der Unterstützung ausgeliefert, und in diesem Kapitel versuchen wir, den Benutzern deren Gebrauch zu erklären.

3.1.2 Die Zugriffskontrollen des Dateisystems

Es ist wichtig festzustellen, dass MS Windows ein völlig anderes Dateizugriffssystem benutzt als UNIX-Systeme. Wir werden erst die Unterschiede erklären und dann zeigen, wie Samba hilft, diese Unterschiede zu überbrücken.

Vergleich zwischen NTFS und dem UNIX-Dateisystem

Samba benutzt das UNIX-Dateisystem, d.h., Samba verhält sich innerhalb der Möglichkeiten des UNIX-Dateisystems. Aber Samba ist auch dafür verantwortlich, das Verhalten des Windows-Dateisystems nachzustellen. Glücklicherweise bietet Samba eine Reihe von Konfigurationsmöglichkeiten, um die Unterschiede zu überbrücken. Wir werden einige dieser Einstellungsmöglichkeiten betrachten,

jedoch nicht alle. Wer mehr wissen möchte, sollte die Manpage der Datei smb.conf lesen. Im Folgenden sehen Sie einen Vergleich des UNIX-Dateisystems mit dem Dateisystem von Windows NT/200x:

Namensraum

Windows-Dateinamen können 254 Zeichen lang sein, UNIX beherrscht bis zu 1023 Zeichen. Die Dateierweiterung beschreibt in Windows einen bestimmten Dateityp, in UNIX-Systemen ist das nicht zwingend so. Was unter Windows ein ‚Ordner' ist, heißt in UNIX ‚Verzeichnis'.

Groß-/Kleinschreibung

Im Allgemeinen sind Dateinamen unter Windows 8+3 Zeichen lang und werden in Großbuchstaben erstellt. Dateinamen, die länger sind, sind in ihrer Schreibweise case-insensitive (d.h., es spielt keine Rolle, ob sie groß- oder kleingeschrieben werden). Unter UNIX sind alle Dateien und Verzeichnisse case-sensitive (d.h., es spielt sehr wohl eine Rolle, ob ein Dateiname groß- oder kleingeschrieben wird). Im folgenden Beispiel würden die Dateinamen von Windows völlig gleich interpretiert werden, für UNIX wären es drei verschiedene Dateien:

```
MYFILE.TXT MyFile.txt myfile.txt
```

Es wird ziemlich klar, dass diese Dateien in Windows nicht nebeneinander (im selben Ordner) stehen könnten, unter ist das UNIX jedoch jederzeit möglich. Was soll nun Samba tun, wenn es auf diese Dateien trifft? Die Lösung besteht darin, dass die erste Datei für Windows-Benutzer sichtbar ist, die anderen jedoch nicht verfügbar bzw. unsichtbar sind; eine andere Lösung ist nicht denkbar.

Verzeichnis-Trennzeichen

MS Windows und DOS benutzen das Zeichen\ (Backslash) als Verzeichnis-Trennzeichen, UNIX benutzt (wie im Internet üblich) den Slash / als Verzeichnis-Trennzeichen. Dies wird von Samba transparent (für den Windows-Benutzer unbemerkt) umgesetzt.

Laufwerksbezeichnung

In MS Windows werden verschiedene Festplatten-Partitionen mit Buchstaben belegt (C:). Es gibt unter UNIX kein ähnliches Konzept, Festplatten-Teile (Partitionen) werden als Teil des Dateisystems eingebunden (gemountet). Was unter DOS C:\ ist, wäre unter UNIX einfach / (root = Wurzel des Dateisystembaums).

Dateinamenskonvention

MS Windows kennt keine Dateien, deren Namen mit einem Punkt beginnen (.). In UNIX werden solche Dateien häufig in den „Home"-Verzeichnissen (Heimatverzeichnissen) von Benutzern gefunden. Punktdateien (.) sind typischerweise Start- oder Konfigurationsdateien für UNIX-Programme.

Verknüpfungen und Verkürzungen

Unter Windows sind Verknüpfungen spezielle Dateitypen, die zum verkürzten Starten von Programmen in deren realen Ordner dienen. Auch unter UNIX gibt es Verknüpfungen und Verkürzungen, diese werden jedoch völlig unterschiedlich gehandhabt. Symbolische Verknüpfungen unter UNIX halten die aktuellen Informationen von Dateien oder Verzeichnissen. Schreib- und Lesezugriffe auf eine Verknüpfung verhalten sich genauso wie bei der originalen Datei. Symbolische Verknüpfungen nennt man auch weiche Verknüpfungen. Harte Verknüpfungen kennt Windows nicht, diese würden das Benutzen ein- und derselben Datei unter mehreren Namen gleichzeitig ermöglichen. Es gibt noch viele Unterschiede, die einem Windows-Administrator unangenehm im Umgang mit UNIX sein könnten.

Verwaltung von Verzeichnissen

Es gibt grundsätzlich drei Möglichkeiten, um Ordner (Verzeichnisse) zu verwalten: `create` (erstellen), `delete` (löschen) und `rename` (umbenennen).

Verwaltung von Ordnern (Verzeichnissen) mit UNIX und Windows

Aktion	Windows-Befehl	UNIX-Befehl
create	md folder	mkdir folder
delete	rd folder	rmdir folder
rename	rename oldname newname	mv oldname newname

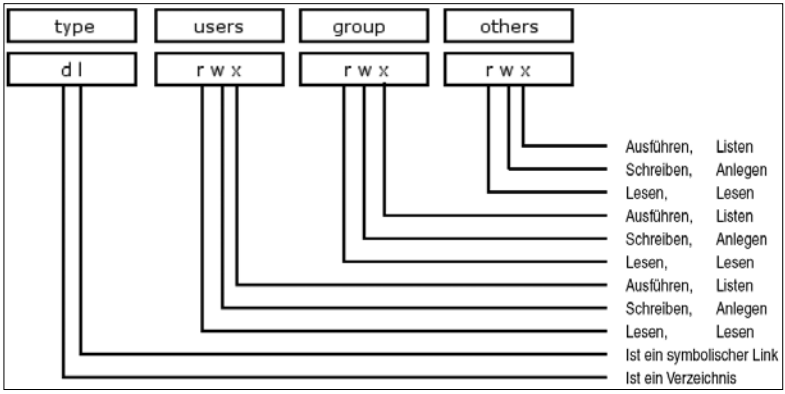
Die Verwaltung der Zugriffskontrollen von Dateien und Ordnern (Verzeichnissen)

Jedem Administrator wird geraten, zusätzlich Handbücher zu diesem Thema zu studieren. Die meisten Fälle können mit den grundlegenden Zugriffsmöglichkeiten von UNIX gelöst werden, ohne die Technologien der Zugriffskontroll-Listen (ACLs) oder der erweiterten Attribute (EAs) zu verwenden. Die Datei- und Verzeichnisverwaltung von UNIX basiert auf folgenden Zugriffsmöglichkeiten:

```
$ls -la
total 632
drwxr-xr-x 13 maryo gnomes 816 2003-05-12 22:56 .
drwxrwxr-x 37 maryo gnomes 3800 2003-05-12 22:29 ..
dr-xr-xr-x 2 maryo gnomes 48 2003-05-12 22:29 muchado02
drwxrwxrwx 2 maryo gnomes 48 2003-05-12 22:29 muchado03
drw-rw-rw- 2 maryo gnomes 48 2003-05-12 22:29 muchado04
d-w--w--w- 2 maryo gnomes 48 2003-05-12 22:29 muchado05
dr--r--r-- 2 maryo gnomes 48 2003-05-12 22:29 muchado06
drwsrwsrwx 2 maryo gnomes 48 2003-05-12 22:29 muchado08
```

```
---------- 1 maryo gnomes 1242 2003-05-12 22:31 mydata00.lst
--w--w--w- 1 maryo gnomes 7754 2003-05-12 22:33 mydata02.lst
-r--r--r-- 1 maryo gnomes 21017 2003-05-12 22:32 mydata04.lst
-rw-rw-rw- 1 maryo gnomes 41105 2003-05-12 22:32 mydata06.lst
$
```

Die Reihen oben repräsentieren (von rechts nach links): die Berechtigung, die Anzahl der „harten“ Links einer Datei, den Besitzer (einer Datei), die Besitzergruppe und die Größe in Bytes.



Rechtestruktur: Übersicht über die UNIX-Berechtigungen.

Jedes Bit kann auch unbesetzt sein und wird durch ein Minus (-) dargestellt.

```
-rwxr-x--- Bedeutet: Der Besitzer kann lesen, schreiben und
ausführen. Die Gruppe kann lesen und ausführen. Andere haben
keine Rechte.
```

Zusätzliche Möglichkeiten im Typen-Feld [type] sind: c = character device, b = block device, p = pipe device, s = UNIX-Domain-Socket. Die Zeichen `rwxXst` für die Berechtigungen für Nutzer, Gruppen und andere sind: lesen (r), schreiben (w), ausführen (oder Ordner-Zugriff) (x), exklusives Ausführen, wenn der Nutzer berechtigt für die Datei oder den Ordner ist (X), Setzen der ID des Nutzers bei Ausführung (s), Sticky-Bit (begleitendes Bit) (t).

Wenn das Sticky-Bit auf einem Verzeichnis gesetzt ist, können darin enthaltene Dateien nur vom Nutzer `root` oder dem Ersteller der Dateien gelöscht werden. In jedem anderem Fall sind alle anderen Dateivorgänge (löschen, lesen, umbenennen) erlaubt. Das Sticky-Bit wird häufig für Verzeichnisse wie das */tmp*-Verzeichnis benutzt, die gewöhnlich für jeden beschreibbar sind. Wenn auf einem Verzeichnis das Gruppen- oder Nutzer-Identitätsbit gesetzt ist, dann erhalten Nutzer und Gruppen Berechtigungen auf darin enthaltene Dateien. Dies ermöglicht das

Erstellen von Verzeichnissen, in denen alle Nutzer einer Gruppe auf eine Datei zugreifen können sollen, insbesondere dann, wenn es nicht erwünscht ist, dass diese Datei exklusiv einem Benutzer gehört, der zu einer anderen primären Gruppe gehört als die übrigen Nutzer.

Falls ein Verzeichnis auf `drw-r-----` gesetzt ist, heißt dies, dass der Eigner in ihm Dateien lesen und schreiben (erstellen) kann, aber dadurch, dass das Ausführen-Flag (x) nicht gesetzt ist, können die Dateien in diesem Verzeichnis von niemandem gesehen werden. Die Gruppe kann Dateien lesen, aber keine neuen anlegen. Falls Dateien in dem Verzeichnis für die Gruppe les- oder schreibbar gesetzt sind, können die Gruppenmitglieder diese schreiben oder löschen.

3.1.3 Zugriffskontrollen für Freigabedefinitionen

Die folgenden Parameter in den Dateisektionen von *smb.conf* definieren eine Freigabekontrolle oder betreffen Zugriffskontrollen. Bevor Sie eine dieser folgenden Optionen benutzen, sehen Sie bitte in den Manpages für *smb.conf* nach.

Benutzer- und gruppen-basierende Kontrollen

Benutzer- und gruppen-basierende Kontrollen können sehr hilfreich sein. In manchen Situationen ist es sogar gewünscht, dass alle Dateisystem-Operationen behandelt werden, als wären sie von einem einzelnen Benutzer durchgeführt worden. Die Benutzung von `force user` und `force group` wird dies erreichen. In anderen Situationen ist es vielleicht notwendig, ein paranoides Maß an Kontrollen einzusetzen, um sicherzustellen, dass es nur bestimmten ausgewählten und autorisierten Personen möglich ist, auf eine Freigabe oder dessen Inhalt zuzugreifen. Hier kann die Benutzung von `valid users` oder `invalid users` am hilfreichsten sein. Wie immer ist es höchst ratsam, die einfachste Methode für die Verwaltung und die eindeutigste Methode für die Zugriffskontrolle zu verwenden. Denken Sie daran, dass nach dem Verlassen Ihrer Arbeit jemand anderes Unterstützung geben können muss, und wenn er eine große Baustelle vorfindet oder Ihre Vorgehensweise nicht versteht, kann es durchaus möglich sein, dass Samba gelöscht wird oder eine alternative Lösung eingesetzt wird.

Benutzer- und gruppen-basierende Kontrollen	
Kontrollparameter	**Beschreibung – Ausführung – Hinweise**
admin users	Liste der Benutzer, denen Administrationsprivilegien auf der Freigabe erteilt werden. Sie werden alle Dateioperationen als Super-User (root) ausführen. Jeder Benutzer in dieser Liste wird in der Lage sein, alles auf der Freigabe zu machen, egal welche Dateiberechtigungen gesetzt wurden.

force group	Spezifiziert einen UNIX-Gruppennamen, der als primäre Standardgruppe allen Benutzern zugewiesen wird, die sich mit diesem Dienst verbinden.
force user	Spezifiziert einen UNIX-Benutzernamen, der als Standardbenutzer allen Benutzern zugewiesen wird, die sich mit diesem Dienst verbinden. Dies ist für das gemeinsame Nutzen von Dateien hilfreich. Die falsche Benutzung kann Sicherheitsprobleme verursachen.
guest ok	Falls dieser Parameter für einen Dienst gesetzt ist, wird kein Passwort verlangt, um sich mit diesem Dienst zu verbinden. Die Privilegien sind diejenigen des Gastzugangs.
invalid users	Liste der Benutzer, denen ein Anmelden an diesem Dienst nicht erlaubt wird.
only user	Kontrolliert, ob Verbindungen mit Benutzernamen, die nicht in der Liste enthalten sind, erlaubt werden.
read list	Liste der Benutzer, die einen Nur-Lesezugriff auf diesen Dienst haben. Benutzer in dieser Liste bekommen keinen Schreibzugriff, egal wie die Option ‚read only' gesetzt wurde.
username	Sehen Sie in der smb.conf-Manpage für mehr Informationen nach -- dies ist ein komplexer Parameter, der häufig falsch angewendet wird.
valid users	Liste der Benutzer, denen das Anmelden an diesem Dienst erlaubt wird.
write list	Liste der Benutzer, denen Lese-Schreibzugriff auf diesen Dienst erlaubt wird.

Kontrollen, die auf Datei- und Verzeichnis-Berechtigungen basieren

Die folgenden auf Datei- und Verzeichnis-Berechtigungen basierenden Kontrollen können, wenn sie falsch angewendet werden, durch Fehlkonfigurationen zu erheblichen Schwierigkeiten bei der Fehlersuche führen. Benutzen Sie diese sparsam und sorgfältig. Durch die schrittweise Einführung einer Berechtigung nach der anderen können unerwünschte Nebeneffekte entdeckt werden. Im Fehlerfall kommentieren Sie alle aus und führen sie dann Schritt für Schritt in einer kontrollierten Art und Weise wieder ein.

Auf Datei- und Verzeichnis-Berechtigungen basierende Kontrollen	
Kontrollparameter	**Beschreibung – Ausführung – Hinweise**
create mask	Sehen Sie in der smb.conf-Manpage nach.
directory mask	Die Oktal-Modi, die beim Konvertieren von DOS-Modi in UNIX-Modi während des Erzeugens von UNIX-Verzeichnissen benutzt werden. Siehe auch: directory security mask.
dos filemode	Durch Einschalten dieses Parameters erlaubt man einem Benutzer, der Schreibzugriff auf eine Datei hat, die Berechtigungen auf diese zu ändern.
force create mode	Dieser Parameter spezifiziert eine Anzahl von UNIX-Mode-Bit-Berechtigungen, die immer auf eine Datei gesetzt werden, die durch Samba erzeugt wurde.
force directory mode	Dieser Parameter spezifiziert eine Anzahl von UNIX-Mode-Bit-Berechtigungen, die immer auf ein Verzeichnis gesetzt werden, das durch Samba erzeugt wurde.
force directory security mode	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen eines Verzeichnisses manipuliert.
force security mode	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen manipuliert.
hide unreadable	Verhindert, dass Clients die Existenz von Dateien sehen, die nicht lesbar sind.
hide unwriteable files	Verhindert, dass Clients die Existenz von Dateien sehen, die nicht schreibbar sind. Nicht beschreibbare Verzeichnisse werden wie gewöhnlich angezeigt.
nt acl support	Dieser Parameter kontrolliert, ob smbd versuchen wird, UNIX-Berechtigungen auf Windows NT-Zugriffsberechtigungslisten zu mappen.
security mask	Kontrolliert Änderungen an UNIX-Berechtigungsbits, wenn ein Windows NT-Client UNIX-Berechtigungen einer Datei manipuliert.

Allgemeine Kontrollen

Das Folgende ist dokumentiert, da es weit verbreitet ist, dass Administratoren unabsichtlich Barrieren beim Einrichten von Dateizugriffen dadurch aufbauen, dass sie die Auswirkungen von Dateieinstellungen in *smb.conf* nicht verstehen.

Andere Kontrollen	
Kontrollparameter	**Beschreibung – Ausführung – Hinweise**
case sensitive, default case, short preserve case	Bedeutet, dass alle Dateinamensanzeigen in case-sensitiver Art erfolgen. Die Dateien werden genau so mit dem exakten Namen angelegt, wie Samba den Dateinamen vom Windows-Client erhält.
csc policy	Client-seitige Caching-Richtlinie – ermöglicht parallele MS Windows client-seitige Datei-Caching-Fähigkeiten.
dont descend	Erlaubt das Spezifizieren einer kommata-getrennten Verzeichnisliste, die der Server immer leer anzeigt.
dos filetime resolution	Diese Option ist hauptsächlich als Kompatibilitätsoption für Visual C++ gedacht, wenn dieses auf einer Samba-Freigabe genutzt wird.
dos filetimes	DOS und Windows erlauben Benutzern, Zeitstempel auf Dateien zu ändern, wenn sie auf die Datei schreiben können. POSIX-Semantiken verhindern dies. Die Option erlaubt DOS- und Windows-Verhalten.
fake oplocks	Oplocks sind das Verfahren, wie SMB-Clients die Erlaubnis eines Servers bekommen, Dateioperationen lokal zu cachen (zwischenzuspeichern). Falls ein Server Oplocks erlaubt, ist es dem Client freigestellt anzunehmen, dass er der einzige ist, der auf die Datei zugreift, und er kann das Datei-Caching aggressiv nutzen.
hide dot files, hide files, veto files	Hinweis: MS Windows Explorer erlaubt das Überschreiben von Dateien, die als versteckt markiert sind, so dass sie weiter sichtbar sind.
read only	Falls dieser Parameter ‚yes' ist, können Benutzer eines Dienstes Dateien im Diensteverzeichnis weder erzeugen noch ändern.
veto files	Liste von Dateien oder Verzeichnissen, die nicht sichtbar sind und auf die man nicht zugreifen kann.

3.1.4 Zugriffskontrollen auf Freigaben

Dieses Kapitel handelt davon, wie Samba für Zugriffskontroll-Einschränkungen bei Freigaben konfiguriert werden kann. Standardmäßig setzt Samba keine Einschränkungen auf die Freigabe selbst. Einschränkungen auf der Freigabe selbst können auf MS Windows NT4/200x/XP-Freigaben gesetzt werden. Dies kann ein effektives Verfahren sein, um zu regeln, wer sich mit einer Freigabe verbinden darf. In Ermangelung spezifischer Einschränkungen sieht die Standardeinstellung vor, dem globalen Benutzer `Jeder - Volle Kontrolle` (volle Kontrolle, Ändern und Lesen) zu erlauben.

Zurzeit stellt Samba kein Werkzeug zum Konfigurieren von Zugriffskontroll-Einstellungen auf einer Freigabe selbst zur Verfügung. Samba hat die Fähigkeit, Zugriffskontroll-Einstellungen zu speichern und damit zu arbeiten, aber der einzige Weg, diese Einstellungen zu erzeugen, ist der NT4 Server Manager oder die Windows 200x MMC für Computer-Verwaltung.

Samba speichert die Zugriffskontroll-Einstellungen pro Freigabe in der Datei *share_info.tdb*. Der Ablageort dieser Datei auf Ihrem System hängt davon ab, wie Sie Samba kompiliert haben. Der Standard-Ablageort für Sambas tdb-Dateien ist */usr/local/samba/var*. Falls das *tdbdump*-Werkzeug auf Ihrem System kompiliert und installiert worden ist, können Sie den Inhalt dieser Datei wie folgt ausführen: `tdbdump share_info.tdb`, in dem Verzeichnis, das die tdb-Dateien enthält.

Verwaltung von Freigabeberechtigungen

Das beste Werkzeug für eine Aufgabe ist plattformabhängig. Wählen Sie das beste Werkzeug für Ihre Umgebung.

Windows NT4 Workstation/Server

Das Werkzeug, das Sie zum Verwalten von Freigabeberechtigungen auf einem Samba-Server nutzen müssen, ist der NT Server Manager. Der Server Manager wird mit den Windows NT4 Server-Produkten, aber nicht mit Windows NT4 Workstation ausgeliefert. Sie können den NT Server Manager für MS Windows NT4 Workstation von Microsoft erhalten (Details weiter unten).

1. Starten Sie den NT4 Server Manager, und klicken Sie auf den Samba-Server, den Sie administrieren möchten. In dem Menü wählen Sie *Computer*, dann klicken Sie auf *Freigegebene Verzeichnisse*.

2. Klicken Sie auf die Freigabe, die Sie verwalten möchten, dann gehen Sie auf *Eigenschaften* und klicken auf die Registerkarte *Berechtigungen*. Jetzt können Sie Zugriffskontroll-Einstellungen nach Belieben hinzufügen und ändern.

Windows XP

Auf MS Windows NT4/XP werden Systemzugriffskontroll-Listen für Freigaben mit eigenen Werkzeugen gesetzt, meist durch den Dateimananger. In Windows

XP beispielsweise rechtsklicken Sie auf den Freigabeordner, wählen *Freigabe* und klicken dann auf *Berechtigungen*. Die Standardberechtigung unter Windows NT4/XP erlaubt „jedem" volle Kontrolle über die Freigabe.

Windows XP und spätere Versionen enthalten das Werkzeug *Computerverwaltungs*-Snap-In für die Microsoft Management Konsole (MMC). Dieses Werkzeug befindet sich in der *Systemsteuerung -> Verwaltung -> Computerverwaltung*.

1. Nachdem Sie die MMC über das *Computerverwaltungs*-Snap-In gestartet haben, klicken Sie auf den Menüeintrag *Action* und wählen dann *Mit einem anderen Computer verbinden*. Falls Sie nicht an einer Domäne angemeldet sind, werden Sie aufgefordert, einen Domänenbenutzer und ein Passwort einzugeben. Dies wird Sie gegenüber der Domäne authentifizieren. Falls Sie bereits als ein Benutzer mit Administrationsrechten angemeldet sind, wird dieser Schritt nicht angeboten.

2. Falls der Samba-Server nicht in der Box *Computer auswählen* angezeigt wird, geben Sie den Namen des Samba-Zielservers im Feld `Name:` ein. Klicken Sie jetzt auf den Button [+] neben Systemwerkzeuge, dann auf den Button [+] neben *Freigabeordner* im linken Bereich.

3. Im rechten Bereich doppelklicken Sie auf die Freigabe, auf die Sie Zugriffskontroll-Berechtigungen vergeben möchten. Dann klicken Sie auf die Registerkarte-Freigabe-Berechtigungen. Jetzt ist es möglich, Zugriffskontroll-Einheiten zu dem Freigabe-Ordner hinzuzufügen. Merken Sie sich, welchen Zugriffstyp (volle Kontrolle, ändern, lesen) Sie für jeden Eintrag vergeben möchten.

Seien Sie vorsichtig: Falls Sie alle Berechtigungen von dem „Jeder"-Benutzer wegnehmen, ohne diesen Benutzer entfernt zu haben, wird anschließend kein Benutzer mehr in der Lage sein, auf die Freigabe zuzugreifen. Dies ist ein Ergebnis dessen, was als ACL-Präzedenz bekannt ist. „Jeder" mit dem Eintrag kein Zugriff heißt, dass „MaryK", die Teil der Gruppe „Jeder" ist, keinen Zugriff hat, obwohl ihr explizit volle Zugriffsrechte gegeben wurden.

3.1.5 MS Windows-Zugriffskontroll-Listen (ACLs) und UNIX-Wechselwirkungen

Verwalten von UNIX-Berechtigungen durch NT-Sicherheitsdialoge

Windows NT-Clients können ihre eigene Dialogbox für Sicherheitseinstellungen verwenden, um UNIX-Berechtigungen anzuzeigen und zu ändern.

Diese Fähigkeit ist so umsichtig, dass die Sicherheit des UNIX-Hosts, auf dem Samba läuft, nicht gefährdet wird und dennoch alle Dateiberechtigungsregeln, die ein Samba-Administrator setzt, beachtet werden.

Samba versucht nicht, die POSIX-ACLs zu übertreffen, so dass die vielen feiner abgestimmten Zugriffskontroll-Optionen, die Windows zur Verfügung stellt, einfach ignoriert werden.

Hinweis: Alle Zugriffe auf UNIX/Linux-Systemdateien durch Samba werden durch die Betriebssystem-Dateizugriffskontrollen kontrolliert. Bei der Fehlersuche nach Dateizugriffsproblemen ist es enorm wichtig, die Identität des Windows-Benutzers herauszufinden, wie sie von Samba an dieser Stelle des Dateizugriffs gesehen wird. Diese lässt sich am besten durch Einsicht in die Samba-Protokolldateien ermitteln.

Anzeigen von Dateisicherheit auf einer Samba-Freigabe

Von einem NT4/2000/XP-Client aus rechtsklicken Sie auf jede Datei oder Verzeichnis in einem Samba-gemounteten Laufwerksbuchstaben oder UNC-Pfad. Wenn das Menü aufgeht, klicken Sie auf den Eintrag *Eigenschaften* am Fuß des Menüs. Dies startet die Dialogbox *Eigenschaften*. Klicken Sie auf die Registerkarte *Sicherheit*, *Erweitert* und Sie werden drei Panels sehen: *Berechtigungen*, *Überwachung* und *Besitzer*. Der Button Überwachung wird entweder eine Fehlermeldung „A requested privilege is not held by the client" verursachen, falls der Benutzer kein NT-Administrator ist, oder einen Dialog erscheinen lassen, mit dem ein Administrator Überwachungsgrundlagen einer Datei hinzufügen kann, wenn der Benutzer als NT-Administrator angemeldet ist. Dieser Dialog funktioniert derzeit nicht mit einer Samba-Freigabe, da der einzige Button, der *Hinzufügen*-Button, es derzeit nicht zulässt, eine Benutzerliste anzuzeigen.

Anzeigen von Dateieigentümern

Wenn Sie auf den Button Eigentümer klicken, erscheint eine Dialogbox, die Ihnen zeigt, wem die betreffende Datei gehört. Der Name des Eigentümers wird wie folgt angezeigt:

```
SERVER\Benutzer (Langer Name)
```

SERVER ist der NetBIOS-Name des Samba-Servers, *Benutzer* der Name des UNIX-Benutzers, dem die Datei gehört, und (*Langer Name*) ist die Beschreibung, die den Benutzer ausweist (normalerweise wird dies im GECOS-Feld der UNIX-Passwortdatenbank gefunden). Klicken Sie auf den Button *Abbrechen*, um diesen Dialog zu entfernen.

Falls der Parameter `nt acl support` auf `false` gesetzt ist, wird der Dateieigentümer als NT-Benutzer „Jeder" angezeigt. Mit dem *Übernehmen*-Button können Sie nicht die Eigentumsrechte an dieser Datei auf sich selbst setzen (ein Anklicken zeigt eine Dialogbox, die angibt, dass der Benutzer, als der Sie gerade auf dem NT-Client angemeldet sind, nicht gefunden werden kann). Der Grund hierfür ist, dass das Ändern der Eigentumsrechte auf eine Datei eine privilegierte Operation in UNIX ist, die ausschließlich dem Benutzer *root* obliegt. Indem Sie auf diesen Button klicken, veranlassen Sie NT dazu, die Eigentumsrechte einer Datei auf den am NT-Client gegenwärtig angemeldeten Benutzer zu übertragen; dies funktioniert jedoch zu diesem Zeitpunkt mit Samba nicht.

Es gibt ein NT-Kommando, *chown*, das mit Samba funktioniert und es einem Benutzer, der mit Administratorprivilegien an einen Samba-Server als *root* angeschlossen ist, erlaubt, die Eigentumsrechte von Dateien sowohl auf lokaler NTFS-Dateisystemebene als auch auf entfernt gemounteten NTFS- oder Samba-Laufwerken zu setzen. Dies ist verfügbar als Teil der von Jeremy Allison vom Samba-Team geschriebenen *Seclib*-NT-Sicherheitsbibliothek, und Sie können es von der FTP-Hauptseite von Samba abrufen.

Das Anzeigen von Datei- oder Verzeichnisberechtigungen

Der dritte Button ist die Schaltfläche *Berechtigungen*. Wenn Sie sie anklicken, öffnet sich eine Dialog, der sowohl die Berechtigungen als auch den UNIX-Besitzer für die Datei und das Verzeichnis anzeigen. Der Eigentümer wird so angezeigt:

```
SERVER\Benutzer (Langer Name)
```

SERVER ist der NetBIOS-Name des Samba-Servers, *Benutzer* ist der Name des UNIX-Benutzers, dem die Datei gehört, und (*Langer Name*) ist die Beschreibung, die den Benutzer ausweist (normalerweise wird dies im GECOS-Feld der UNIX-Passwortdatenbank gefunden). Falls der Parameter `nt acl support` auf `false` gesetzt ist, wird der Dateieigentümer als NT-Benutzer „Jeder“ angezeigt. Das Berechtigungsfeld wird bei Dateien und Verzeichnissen anders dargestellt, also werde ich die Art, wie Dateiberechtigungen angezeigt werden, zuerst beschreiben.

Dateiberechtigungen

Die Standard-UNIX-Drillinge Benutzer/Gruppe/Welt und die korrespondierenden Berechtigungen lesen, schreiben, ausführen werden von Samba in ein aus drei Elementen bestehendes NT-ACL mit den Bits `r`, `w` und `x` von Samba in ein aus drei Elementen bestehendes NT-ACL gemappt, wobei die Bits `r`, `w` und `x` auf passende NT-Berechtigungen gemappt werden. Die UNIX-Welt-Berechtigungen werden in die globale NT-Gruppe „Jeder“ gemappt, gefolgt von der Berechtigungsliste, die unter UNIX für Welt gilt. Die UNIX Eigentümer- und Gruppenberechtigungen werden als ein NT-*Benutzer*-Symbol und ein NT-Symbol *lokale Gruppe* angezeigt, beziehungsweise durch die nachfolgende Berechtigungsliste für den UNIX-Benutzer und die UNIX-Gruppe.

Dadurch, dass viele UNIX-Berechtigungssätze nicht auf allgemeine NT-Namen wie lesen, ändern oder volle Kontrolle passen, werden gemeinhin die Berechtigungen durch Wörter wie *Spezieller Zugriff* in der NT-Anzeigeliste angeführt.

Doch was passiert, wenn die Datei keine Berechtigungen für eine bestimmte UNIX-Benutzergruppe oder Welt-Komponente erlaubt? Um es zu ermöglichen, keine Berechtigungen zu sehen und zu ändern, übergibt Samba das NT-ACL-Attribut *Eigentum übernehmen* (das keine Bedeutung für UNIX hat) und meldet eine Komponente ohne Berechtigung, wie wenn das NT-Bit O gesetzt wäre. Dies wurde natürlich deshalb gewählt, um es wie eine Null aussehen zu lassen, was bedeutet: Keine (Null) Berechtigungen.

Verzeichnis-Berechtigungen

Verzeichnisse auf einem NTFS-Dateisystem haben zwei verschiedene Berechtigungssätze. Der erste Satz ist die ACL, die auf das Verzeichnis selbst gesetzt ist. Sie wird normalerweise im ersten Satz der Klammern im normalen NT-Stil `RW` angezeigt. Dieser erste Satz an Berechtigungen wird durch Samba in exakt derselben Art und Weise erzeugt, wie es normale Dateiberechtigungen werden, und wird auch auf dieselbe Art und Weise angezeigt. Der zweite Satz von Verzeichnis-Berechtigungen hat keine echte Bedeutung in der UNIX-Berechtigungs-Welt und repräsentiert die vererbten Berechtigungen, die jede Datei erben würde, die in diesem Verzeichnis erzeugt wird. Samba vereinigt diese vererbten Berechtigungen für NT, indem es die UNIX-Berechtigungsmodi als eine NT-ACL zurückgibt, so wie es eine Datei erhalten würde, die Samba für diese Freigabe erzeugt hat.

Ändern von Datei- oder Verzeichnis-Berechtigungen

Das Ändern von Datei- und Verzeichnis-Berechtigungen ist genauso einfach wie das Ändern der Anzeige der Berechtigungen in der Dialogbox und das Klicken auf OK. Jedoch gibt es Einschränkungen, die ein Benutzer kennen sollte und die mit den Standard-Samba-Berechtigungsmasken und mit dem Vergeben von DOS-Attributen zu tun haben, die ebenfalls in diesem Zusammenhang berücksichtigt werden müssen. Falls der Parameter `nt acl support` auf `false` gesetzt ist, schlägt jeder Versuch, Sicherheitsberechtigungen zu setzen, mit einer Meldung „Zugriff verweigert“ fehl.

Das Erste, was anzumerken ist, ist, dass der Button Hinzufügen keine Samba-Benutzerliste zurückgeben wird (es wird eine Fehlermeldung ausgegeben, die besagt „Der Remoteprozedur-Aufruf schlug fehl und konnte nicht ausgeführt werden“). Das bedeutet, dass Sie nur die gegenwärtigen Benutzer/Gruppen/Welt-Berechtigungen, die im Dialog angezeigt werden, ändern können. Dies funktioniert gut, weil es die einzigen Berechtigungen sind, die UNIX augenblicklich hat.

Falls ein Berechtigungsdrilling (entweder Benutzer, Gruppe oder Welt) von der Liste der Berechtigungen in der NT-Dialogbox entfernt wird und dann der OK-Button angeklickt wird, wird dies auf UNIX-Seite als *keine Berechtigungen* angewendet. Wenn Sie sich dann die Berechtigungen nochmals ansehen, wird der Eintrag *keine Berechtigungen* als das NT-Flag O wie oben beschrieben angezeigt. Dies erlaubt es Ihnen, Berechtigungen wieder auf eine Datei oder Verzeichnis zu setzen, nachdem Sie diese von einer der Drillingskomponenten entfernt hatten.

Weil UNIX nur die Bits `r`, `w` und `x` einer NT-ACL unterstützt, werden diese ignoriert, falls andere NT-Sicherheitsattribute wie *Löschzugriff* ausgewählt wurden, falls diese auf einem Samba-Server angewandt werden.

Wenn Berechtigungen auf ein Verzeichnis gesetzt werden, wird der zweite Satz an Berechtigungen (im zweiten Klammern-Paar) standardmäßig auf alle Dateien in diesem Verzeichnis angewandt. Falls Sie dies nicht wünschen, müssen Sie die Auswahlbox *Berechtigungen auf existierende Dateien zurücksetzen* in dem NT-Dialog vor einem Klicken auf OK abwählen.

Falls Sie es wünschen, alle Berechtigungen von einer Benutzer/Gruppe/Welt-Komponente zu entfernen, können Sie entweder eine Komponente auswählen und auf den Button *Entfernen* klicken, oder setzen Sie die Komponente darauf, nur die spezielle Berechtigung *Berechtigung übernehmen* (angezeigt als O) zu setzen.

Die Wechselwirkung mit den Samba-Standard-Parametern create mask

Es gibt vier Parameter, die das Wechselspiel mit den Samba-Standard-Parametern `create mask` kontrollieren. Diese sind:

- security mask
- force security mode
- directory security mask
- force directory security mode

Sobald ein Benutzer auf OK klickt, um Berechtigungen zu setzen, mappt Samba die angegebenen Berechtigungen in einen Benutzer/Gruppe/Welt-Drillingssatz und gleicht dann die geänderten Berechtigungen für diese Datei mit den in `security mask` gesetzten Bits ab. Jedes geänderte Bit, das nicht mit 1 in diesem Parameter gesetzt wurde, bleibt in den Dateiberechtigungen unberücksichtigt. Grundsätzlich werden Null-Bits in der `security mask` als ein Satz von Bits behandelt, die der Benutzer *nicht* ändern darf, Einer-Bits darf der Benutzer ändern.

Falls er nicht ausdrücklich gesetzt worden ist, zeigt dieser Parameter standardmäßig auf denselben Wert wie der Parameter `create mask`. Um es einem Benutzer zu erlauben, alle Berechtigungen von Benutzer/Gruppe/Welt an einer Datei zu ändern, setzen Sie diesen Parameter auf 0777.

Als Nächstes gleicht Samba die geänderten Berechtigungen einer Datei mit den Bits ab, die im `force security mode`-Parameter gesetzt sind. Jedes geänderte Bit wird passend zu den auf `1` gesetzten Bits in diesem Parameter zwangsläufig gesetzt. Grundsätzlich werden Bits aus dem Parameter `force security mode` als ein Satz von Bits behandelt, die der Benutzer immer auf „an“ gesetzt hat, wenn die Sicherheit einer Datei geändert wird.

Falls er nicht ausdrücklich gesetzt worden ist, zeigt dieser Parameter standardmäßig auf denselben Wert wie der Parameter `force create mode`. Um es einem Benutzer zu erlauben, alle Berechtigungen von Benutzer/Gruppe/Welt an einer Datei ohne Berechtigungen zu ändern, setzen Sie diesen Parameter auf 000. Die Parameter `security mask` und `force security mode` werden angewendet, um die Anfragen in dieser Reihenfolge zu ändern. Für ein Verzeichnis wird Samba dieselben Operationen durchführen, wie zuvor für eine Datei beschrieben. Es wird jedoch der Parameter `directory security mask` anstatt des Parameters `security mask` und Parameter `force directory security mode` anstatt des Parameters `force security mode` angewandt.

Der Parameter `directory security mask` ist standardmäßig auf denselben Wert wie der Parameter `directory mask` gesetzt, und der Parameter `force directory security mode` ist standardmäßig auf denselben Wert wie der Para-

meter `force directory mode` gesetzt. Auf diese Weise erzwingt Samba die Einschränkungen bei Berechtigungen, die ein Administrator auf einer Samba-Freigabe gesetzt hat, während den Benutzern weiterhin erlaubt wird, innerhalb dieser Einschränkung die Berechtigungsbits zu ändern.

Falls Sie eine Freigabe aufsetzen möchten, die es Benutzern erlaubt, die volle Kontrolle bei der Änderung von Berechtigungsbits auf ihren eigenen Dateien und Verzeichnissen auszuüben, und die es nicht erfordert, irgendwelche Bits auf „an" zu verstellen, dann setzen Sie die folgenden Parameter in der *smb.conf* Datei innerhalb des freigabe-spezifischen Abschnitts:

```
security mask = 0777
force security mode = 0
directory security mask = 0777
force directory security mode = 0
```

Die Wechselwirkung mit den Standard-Samba-Dateiattribut-Vergaben

Hinweis: Samba vergibt einige der DOS-Attribut-Bits (wie z.B. Nur lesen) in den UNIX-Berechtigungen einer Datei. Dies bedeutet, dass es einen Konflikt zwischen den Berechtigungsbits, die durch den Sicherheitsdialog gesetzt wurden, und den Berechtigungen geben kann, die durch die Vergabe von Dateiattributen gesetzt wurden.

Falls eine Datei für den Eigentümer keinen UNIX-Lesezugriff hat, wird diese als „Nur lesen" in dem Standarddialog der Registerkarte *Dateiattribute* angezeigt. Leider ist dieser Dialog derselbe, der die Sicherheitsinformationen in einer anderen Registerkarte enthält. Der Eigentümer kann dadurch fälschlicherweise glauben, die Berechtigungen dadurch ändern zu können, weil es ihm anscheinend erlaubt wird, Lesezugriff durch Nutzung des Sicherheitsdialoges zu bekommen; er klickt auf OK, um zurück zu der Registerkarte mit den Standardattributen zu gelangen, klickt auf OK in diesem Dialog, und NT setzt die Dateiberechtigungen auf Nur-lesen zurück (weil dies die Attribute in diesem Dialog ihm sagen). Dies bedeutet: Klicken Sie – nachdem Sie die Berechtigungen gesetzt und auf OK zum Zurückgehen auf den Attributdialog geklickt haben – immer auf Abbrechen statt auf OK, um sicherzustellen, dass Ihre Änderungen nicht überschrieben werden.

3.1.6 Gängige Fehler

Datei-, Verzeichnis- und Freigabezugriffsprobleme tauchen oft auf der Mailingliste auf. Die folgenden Beispiele wurden kürzlich in der Mailingliste behandelt.

Benutzer können nicht auf eine öffentliche Freigabe schreiben

Wir haben einige Schwierigkeiten mit Datei/Verzeichnis-Berechtigungen. Ich kann mich als Admin-User (`root`) an einer Domäne anmelden, und es gibt eine öffentliche Freigabe, auf der jeder die Berechtigung zum Erzeugen und Ändern

von Dateien haben sollte, aber nur `root` kann Dateien ändern, sonst niemand. Wir müssen dauernd auf dem Server `chgrp -R users *` und `chown -R nobody *` eingeben, um den anderen Benutzern das Ändern von Dateien zu erlauben. Es gibt viele Möglichkeiten, dieses Problem zu lösen, und hier sind einige Hinweise:

Gehen Sie auf die oberste Ebene des Verzeichnisses, das freigegeben ist. Setzen Sie die Benutzer und Gruppe als Eigentümer auf das, was öffentlich sein soll:

```
$find ,directory_name‘ -type d -exec chown user.group {}\;
$find ,directory_name‘ -type d -exec chmod 6775 ,directory_
➥ name‘
$find ,directory_name‘ -type f -exec chmod 0775 {} \;
$find ,directory_name‘ -type f -exec chown user.group {}\;
```

Das oben Aufgeführte setzt das Sticky-Bit auf alle Verzeichnisse. Lesen Sie in Ihren UNIX/Linux-Manpages nach, was dies bewirkt. Es veranlasst das Betriebssystem, auf alle Dateien in Ihren Verzeichnissen den Eigentümer des Verzeichnisses zu setzen. Das Verzeichnis heißt: */foobar*

```
$chown jack.engr /foobar
```

Dies ist dasselbe wie:

```
$chown jack /foobar
$chgrp engr /foobar
```

Geben Sie jetzt Folgendes ein:

```
$chmod 6775 /foobar
$ls -al /foobar/..
```

Dann sollten Sie dies sehen:

```
drwsrwsr-x 2 jack engr 48 2003-02-04 09:55 foobar
```

Geben Sie jetzt dies ein:

```
$su - jill
$cd /foobar
$touch Afile
$ls -al
```

Sie sollten nun sehen, dass die Datei Afile, die von Jill erzeugt worden ist, die Eigentumsrechte und Berechtigungen von Jack hat, so wie hier:

```
-rw-r--r-- 1 jack engr 0 2003-02-04 09:57 Afile
```

Fügen Sie jetzt in Ihrer *smb.conf* für die Freigabe Folgendes ein:

```
force create mode=0775
force directory mode=6775
```

Diese Maßnahmen werden nur dann gebraucht, wenn Ihre Benutzer nicht Mitglied der Gruppe sind, die Sie benutzt haben. Das ist dann der Fall, wenn Sie innerhalb des Betriebssystems keine Schreibberechtigung auf das Verzeichnis haben. Alternativ setzen Sie in der *smb.conf* diesen Eintrag für die Freigabe:

```
force user=jack
force group=engr
```

Dateioperationen, die als root mit force user ausgeführt wurden

Wenn Sie einen Benutzer in admin users haben, wird Samba für diesen Benutzer Dateioperationen immer als root ausführen, sogar wenn force user gesetzt wurde.

MS Word mit Samba ändert den Eigentümer einer Datei

Wenn Benutzer B ein Word-Dokument abspeichert, das Benutzer A gehört, ist anschließend der Eigentümer der aktualisierten Datei Benutzer B. Warum macht Samba das? Wie kann ich das beheben?

Word macht Folgendes, wenn Sie ein Word-Dokument ändern: Es erzeugt ein NEUES Dokument mit einem temporären Namen. Word schließt dann das alte Dokument und löscht es. Dann benennt Word das neue Dokument in den Original-Dateinamen um. Es gibt keinen Mechanismus, durch den Samba in irgendeiner Weise wissen kann, dass das neue Dokument wirklich dem Eigentümer der Originaldatei gehören sollte. Samba hat keine Möglichkeit zu erfahren, dass MS Word die Datei umbenannt hat. Samba ist nur in der Lage zu sagen, dass die Datei, die erzeugt wurde, eine NEUE Datei ist, aber nicht, dass die Applikation (Word) diese aktualisiert hat.

Es gibt einen Workaround, um diese Berechtigungsprobleme zu lösen. Dieser Workaround setzt voraus, dass Sie verstehen, wie Sie das Verhalten des Dateisystems innerhalb der Datei *smb.conf* steuern können, und wissen, wie ein UNIX-Dateisystem funktioniert. Setzen Sie `chmod g+s directory_name` auf das Verzeichnis, in dem Sie Word-Dokumente ändern möchten. Dies stellt sicher, dass alle Dateien mit der Gruppe erzeugt werden, der das Verzeichnis gehört. In dem Abschnitt in der *smb.conf*, der die Freigabe deklariert, setzen Sie:

```
force create mode=0660
force directory mode=0770
```

Diese beiden Einstellungen stellen sicher, dass alle Verzeichnisse und Dateien, die in der Freigabe erzeugt werden, durch den Eigentümer und die Gruppe les- und schreibbar sind, die auf das Verzeichnis selbst gesetzt sind. (mha)

Weiterführende Infos

Dieser Beitrag stammt aus dem Buch „Samba 3 - das offizielle Handbuch“ aus dem Verlag Addison-Wesley. Das Buch in gedruckter Form können Sie unter www.informit.de in unserem Buchshop zum Preis von 59,95 Euro bestellen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Zugriffskontrolle bei Samba und *nix	438639	S.151
Linux als PDC mit Samba 3	402321	–
Linux als Windows-Server mit Samba	402262	–

Mit den Webcodes gelangen Sie auf www.tecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code in das Feld „Webcode“ in der Titelleiste von www.tecChannel.de ein. Es ist möglich, dass Artikel zunächst exklusiv in tecCHANNEL-Compact veröffentlicht werden und daher erst später über den Webcode erreichbar sind.

3.2 Systemsicherheit unter Debian GNU/Linux

Kein Betriebssystem ist vor unbefugten Zugriffen sicher. Auf den folgenden Seiten erfahren Sie, wie man ein Debian-GNU/Linux-System besser gegen solche unberechtigten Attacken schützen. Debian GNU/Linux bietet hierzu einige vorbereitete Pakete, die mit wenig Aufwand zu installieren oder zu konfigurieren sind.

Zunächst sollten Sie bereits bei der Installation des Systems besonders darauf achten, dass Sie sowohl die Frage nach der Verwendung von Shadow-Passwörtern als auch die Frage nach MD5-verschlüsselten Passwörtern mit "Ja" beantworten.

Generell ist zu sagen, dass jeder auf einem Unix-beziehungsweise Linux-System laufende Dienst ein Sicherheitsrisiko darstellen kann. Installieren Sie also ausschließlich nur die Dienste, die auch auf dem System eingesetzt werden sollen.

Das Debian-Team nimmt die Sicherheit des Systems sehr ernst. Sicherheitslücken werden umgehend beseitigt, und aktualisierte Versionen der Softwarepakete sind auf den Debian-FTP-Servern verfügbar. Um Zugriff auf die jeweils aktuellen Sicherheitsupdates zu haben, sollten Sie folgende Zeile der Datei */etc/apt/sources.list* hinzufügen:

```
deb http://security.debian.org/ stable/updates main contrib
non-free
```

3.2.1 Das Paket task-harden

Um sicherzustellen, dass sich keine Pakete mit Sicherheitslücken auf dem System befinden, kann das Paket *task-harden* installiert werden. In diesem Paket sind verschiedene Task-Pakete aufgeführt, die wiederum mit entsprechenden Anhängigkeiten belegt sind. Die „harden-Pakete" werden laufend aktualisiert und, sicherheitskritische Software wird durch entsprechende Abhängigkeiten, die in diesen Paketen festgelegt sind, von der Verwendung ausgeschlossen. Es kann also durchaus passieren, dass die Installation dieses Pakets dazu führt, dass ein benötigter Dienst gelöscht wird. Das Debian-Team ist dabei der Meinung, dass es besser ist, einen Dienst eine Zeit lang nicht zur Verfügung zu stellen, statt einem Angreifer einen Angriffspunkt zu liefern.

Das Paket *task-harden* besitzt definierte Abhängigkeiten zu diversen anderen Paketen, die auch gesondert installiert werden können. Diese decken kleinere Bereiche ab, so dass es möglich ist, einzelne Dienste oder bestimmte Systeme gezielt zu schützen. Diese Pakete sind:

harden – Makes your system hardened.

harden-3rdflaws – Avoid packages with security problems.

harden-clients – Avoid clients that are known to be insecure.

harden-development – Development tools for creating more secure programs.

harden-doc – Useful documentation to secure a Debian system.

harden-environment – Hardened system environment.

harden-localflaws – Avoid packages with security holes.

harden-nids – Harden a system by using a network intrusion detection system.

harden-remoteaudit – Audit your system from this host.

harden-remoteflaws – Avoid packages with security holes.

harden-servers – Avoid servers that are known to be insecure.

harden-surveillance – Check services and/or servers automaticly.

harden-tools – Tools to enhance or analyze the security of the local system.

Die durch diese Systempakete vorgenommenen teilweise tiefgreifenden Veränderungen basieren auf den im Securing Debian HOWTO beschriebenen Aktionen.

3.2.2 Securing Debian HOWTO

Im „Securing Debian HOWTO (http://www.debian.org/doc/manuals/securing-debian-howto/)“ finden sich Informationen darüber, an welchen Stellen ein Debian-System noch sicherer gemacht werden kann. Daher soll an dieser Stelle nur auf einige grundlegende Dinge hingewiesen werden.

Zunächst müssen Sie sich darüber im Klaren sein, dass ein System nur dann hundertprozentig sicher ist, wenn keinerlei Dienste auf diesem nach außen hin über das Netzwerk angeboten werden oder sogar gar keine Verbindung zu einem Netzwerk besteht. Dies ist heutzutage in der Realität natürlich unsinnig und nicht durchsetzbar; das System würde so nicht sinnvoll benutzbar sein. Sie sollten sich auch darüber im Klaren sein, dass die Anforderungen an die Sicherheit stark vom Einsatz des Systems abhängig sind. Ein Privatnutzer wird deutlich andere Anforderungen stellen als der Administrator eines Firewall-Systems. Viele Einstellungen, die die Sicherheit eines Systems erhöhen, vereinfachen den Gebrauch nicht unbedingt; auch hier ist zwischen Benutzbarkeit und Paranoia abzuwägen.

Die softwareseitigen Einstellungen an einem Debian-System, die zur Verbesserung der Sicherheit dienen, können nicht den physikalischen Zugriff auf das System verhindern. Wenn von Systemsicherheit die Rede ist, muss auch bedacht werden, dass zu einem völlig sicheren System auch gehört, dass der Zugriff auf die Hardware unterbunden wird. Ein Angreifer, der Zugriff auf die Hardware hat, kann beispielsweise über eine Boot-CD oder -Diskette Zugriff auf das System erlangen. Auch ein BIOS- oder LILO-Passwort kann den Diebstahl der Festplatte nicht verhindern. Ein völlig sicheres System gehört also hinter gut verschlossene Türen. Doch Betrachtungen zur Hardwaresicherung sollen an dieser Stelle nicht weiter verfolgt werden.

Wichtige Security-Aspekte

Allgemein formuliert sollten folgende Punkte beachtet werden:

1. Entscheiden Sie, welche Dienste auf dem System benötigt werden, und beschränken Sie den Einsatz genau auf diese Dienste – nicht mehr und nicht weniger. Nicht benötigte Dienste sollten auf dem System nicht installiert oder zumindest deaktiviert sein. Weiterhin sollten die benutzten Ports durch eine Firewall auf dem System freigegeben beziehungsweise sollten die Ports von nicht genutzten Diensten über die Firewall gesperrt werden.

2. Verwendete Systemdienste sind speziell abzusichern, so dass bei einem erfolgreichen Angriff auf diesen Dienst nicht das gesamte System kompromittiert wird (beispielsweise durch die Verwendung einer chroot-Umgebung).

3. Auf dem System sollten nur die notwendigen Benutzerkonten angelegt und aktiviert sein. Aktive Benutzerkonten sind durch entsprechende Beschränkungen (Unix-Zugriffsrechte, Quota, ACLs) abzusichern.

4. Setzen Sie Programme ein, die einen unbefugten Zugriff auf das System erkennen und melden, so dass geeignete Gegenmaßnahmen ergriffen werden können.

3.2.3 BIOS-Einstellungen vor der Installation

Bereits vor der Installation können einige wesentliche Maßnahmen zur Sicherheit des Systems getroffen werden. Das Debian-Installationsprogramm enthält ebenfalls einige Punkte, an denen die Sicherheit des Systems verbessert werden kann.

Bevor ein Betriebssystem auf einem neuen Computer installiert wird, sollte ein BIOS-Passwort gesetzt werden, und die Booteinstellungen sollten so gewählt werden, dass ein Systemstart von Diskette nicht möglich ist. Nach der Installation sollte darauf geachtet werden, dass so schnell wie möglich auch der Start von CD-ROM abgeschaltet wird.

Ein weiterer Vorteil dieser Einstellungen zeigt sich, wenn das System als Server in einem Rechenzentrum betrieben wird. Es wäre nicht das erste Mal, dass eine vergessene Diskette im Laufwerk einen erfolgreichen Reboot eines Systems verhindert; und das wird sehr ärgerlich, wenn ein direkter Zugriff auf das System nur mit einer längeren Anfahrt möglich ist.

3.2.4 Festplattenpartitionen

Die endgültige Einteilung des verfügbaren Festplattenplatzes hängt von der Verwendung des Systems ab. Hierzu sollten Sie einige essentielle Dinge beachten:

Jede Partition, auf die die Benutzer des Systems Schreibzugriff haben, sollte auf einer eigenen Partition liegen, beispielsweise in den Bereichen */home* und */tmp*. Dies verhindert, dass ein Benutzer mit oder ohne Absicht das Root-Dateisystem (/) unbenutzbar macht und das gesamte System in einen instabilen Zustand bringt.

Es bleibt natürlich ein gewisser Platz (meist fünf Prozent, dieser Wert kann mit *tunefs* individuell angepasst werden) für den Administrator reserviert, doch kann so anderen Benutzern das Arbeiten mit dem System unmöglich gemacht werden.

Es sollte für jeden Bereich, der automatisch mit Daten gefüllt wird (beispielsweise */var* und hier insbesondere das Verzeichnis */var/log*), eine eigene Partition vorgesehen werden. Auf Debian-Systemen sollte */var* großzügiger bemessen werden, da unter */var/cache/apt/archives* Pakete temporär abgelegt werden, wenn die Installation über das Netz erfolgt. Weiterhin finden sich unter */var/lib/dpkg* viele Dateien, die für das Paketmanagement benötigt werden.

Wenn Software installiert werden soll, die nicht in der Debian-Distribution enthalten ist, sollten auch diese Bereiche auf eigenen Partitionen liegen; diese werden dann bei einer Neuinstallation des Systems nicht überschrieben. Nach dem „File Hierarchy Standard“ (FHS) sind dies */opt* oder */usr/local*.

3.2.5 Administrator Passwort

Während der Installation wird nach einem Passwort für den Administrator (root) gefragt. Zusätzlich kann ein Konto für einen „normalen“ Benutzer dem System hinzugefügt werden; auch für diesen ist dann ein Passwort einzugeben. Auch wenn es möglich ist, hier ein sehr einfaches Passwort zu verwenden, so ist dies natürlich nicht empfehlenswert. Die Auswahl eines guten Passworts ist auf vielen Webseiten im Netz beschrieben, es sind dabei nur einige einfache Regeln zu beachten. Eine Internet-Suche nach „auswahl gutes passwort“ mittels der Suchmaschine Google führt schnell zum Erfolg.

Grundsätzlich sollte auf jedem System neben dem Zugangskonto für den Administrator auch mindestens ein solches Konto für einen Benutzer angelegt werden, das nicht über alle Rechte verfügt. Dieses Benutzerkonto sollte für grundsätzlich alle Logins beziehungsweise Arbeiten auf dem System verwendet werden. Nur wenn für eine bestimmte Aufgabe die Zugriffsrechte nicht ausreichend sind, sollten Sie mit dem Kommando su die Identität auf dem Rechner wechseln. Nach Beendigung der Arbeiten als Administrator sollten Sie sich umgehend wieder als „normaler“ Benutzer im System bewegen.

3.2.6 Passwörter und aktivierte Dienste

Während der Installation erfolgt eine Abfrage, ob „Shadow Passwords“ aktiviert werden sollen. Wenn die Frage positiv beantwortet wird, werden die Passwörter in der Datei */etc/shadow* verschlüsselt gespeichert. Diese Datei kann nur vom Administrator und der Gruppe „shadow“ gelesen werden; somit kann kein Benutzer des Systems die verschlüsselten Passwörter lesen und versuchen, diese mit Hilfe einer Software zu entschlüsseln. Diese Einstellung kann später mit dem Programm *shadowconfig* rückgängig gemacht werden.

Weiterhin besteht die Möglichkeit, die diversen auf dem Rechner abgelegten Passwörter mit einer MD5-Verschlüsselung zu speichern; dies ist generell eine gute Idee, da so ein Angriff erschwert wird und längere Passwörter möglich sind.

Aktivierte Dienste

Wie bereits beschrieben, sollten nur die absolut notwendigen Dienste auf einem System aktiviert werden. Jeder neue Dienst schafft möglicherweise ein neues Sicherheitsloch, das vielleicht erst später zu einem größeren Problem wird. Werden bestimmte Dienste nur selten benötigt, so können diese über die Update-Kommandos (beispielsweise *update-inetd*) gezielt aktiviert und deaktiviert werden.

3.2.7 Mailinglisten

Lesen Sie die Debian-Security-Mailinglisten. Informationen zu den verfügbaren Listen finden Sie auf der debian.org-Homepage (lists.debian.org/debian-security-announce/). Dort ist auch beschrieben, wie Sie sich an einer solchen Liste an- und abmelden. Relevant sind in diesem Zusammenhang *debian-security-announce*, dort werden Sicherheitslücken bekannt gegeben, und Sie werden über Bugfixes dagegen informiert. Eine weitere brauchbare Mailingliste zum Thema ist *debian-security@lists.debian.org*, dort werden viele relevante Sicherheitsthemen rund um Debian detailliert behandelt.

Wenn Sie Meldungen über Sicherheitsupdates per E-Mail bekommen wollen, so senden Sie eine Mail an: *debian-security-announce-request@lists.debian.org* mit dem Wort „subscribe“ im Betreff der Mail. Die Anmeldung an dieser Mailingliste ist auch über die Webseite http://www.debian.org/MailingLists/subscribe möglich. Auf dieser Mailingliste erhalten Sie nur sehr wenige Mails, Sie werden dort aber schnell über Probleme mit Paketen informiert und erfahren eine Internet-Adresse, unter der eine fehlerbereinigte Version des Pakets zur Verfügung steht.

3.2.8 Absicherung des Bootloaders

Nachdem das System mit allen benötigten Programmen eingerichtet ist, kann mit einigen weiteren Aktionen die Sicherheit des Systems weiter erhöht werden. Jede Person, die Zugang zur Tastatur des Systems hat, kann eine Administrator-Shell bekommen und beispielsweise alle Passwörter ändern, indem am Bootprompt `dateiname- des-bootkernels init=/bin/sh` eingegeben wird. Um dies zu verhindern, kann ein Passwort für den Boot-Loader gesetzt werden. Dies kann global für alle Boot-Images geschehen oder individuell für jedes einzelne. Wenn Lilo als Bootloader verwendet wird, muss die Datei */etc/lilo.conf* um die Einträge *password* und *restricted* erweitert werden:

```
image=/boot/2.2.14-vmlinuz
          label=Linux
```

```
read-only
password=hackme
restricted
```

Danach muss *lilo* noch einmal aufgerufen werden. Sorgen Sie dafür, dass die Datei */etc/lilo.conf* nur vom Administrator gelesen werden kann, da das Passwort unverschlüsselt in der Konfigurationsdatei steht; dies erreichen Sie mit dem Kommando `chmod 600 /etc/lilo.conf`. Die Option *restricted* bewirkt, dass nur nach einem Passwort gefragt wird, wenn der Benutzer versucht, zusätzliche Parameter am Bootprompt anzugeben. Die Auswahl verschiedener, bereits in der Konfiguration eingetragener Kernel ist weiterhin möglich. Wird der Eintrag *restricted* weggelassen, fragt Lilo immer nach einem Passwort. Die genannten Einträge können am Anfang der Konfigurationsdatei allgemein gültig für alle Kernel in der Konfiguration angegeben werden oder aber innerhalb eines Abschnitts der Konfigurationsdatei nur für bestimmte Kernel. Wird auf dem System GRUB verwendet, müssen folgende Zeilen der Datei */boot/grub/menu.lst* hinzugefügt werden:

```
timeout 3
password hackme
```

Die Option *timeout* sorgt nach der angegebenen Zeit dafür, dass der Standardeintrag des Systems beim Hochfahren des Rechners gebootet wird.

3.2.9 Starten von Diskette

Der von Debian-Versionen vor 2.2 installierte MBR (Master Boot Record) wurde mit einer Option installiert, die es erlaubte, von Diskette zu booten, auch wenn dies sonst abgeschaltet war. Ob ein solcher MBR installiert ist, lässt sich wie folgt prüfen: Drücken Sie während des Startvorgangs die „↑“-Taste; der MBR-Prompt sollte erscheinen. Drücken Sie nun „f“, und das System startet von Diskette. Mit dieser kann ein Administratorzugang zum System erreicht werden. Dieses Verhalten kann wie folgt verändert werden:

```
lilo -b /dev/hda
```

(wobei *hda* dem entsprechenden Devicenamen Ihres Systems expliziet angepasst werden muss). Die Bootdisketten ab Debian-Version 2.2 installieren lilo direkt in den Master Boot Record (MBR); hier tritt diese Sicherheitslücke nicht auf.

3.2.10 Mounten von Dateisystemen

Beim Mounten (Einhängen in das Dateisystem) von *ext2*-Partitionen gibt es diverse Optionen zu berücksichtigen, die dem Kommando mount übergeben werden oder die direkt in die Datei */etc/fstab* eingetragen werden können. Ein solcher Eintrag könnte beispielsweise wie folgt aussehen:

```
/dev/hda7  /tmp  ext2  defaults,nosuid,noexec,nodev  0  2
```

Die Optionen finden sich in der vierten Spalte. Die Option *nosuid* ignoriert gesetzte SUID- und GUID-Bits auf dieser Partition. Eine gesetzte Option *noexec* verhindert, dass auf dieser Partition befindliche Programme ausgeführt werden können, und *nodev* ignoriert Device-Dateien. Dabei ist zu beachten: Dies bezieht sich nur auf ext2-Dateisysteme. Auch solche Optionen können relativ leicht umgangen werden. Hierzu ein klienes Beispiel:

```
fr@sushi:/tmp# mount | grep tmp
/dev/hda3 on /tmp type ext2 (rw,noexec,nosuid,nodev)
fr@sushi:/tmp# ./date
bash: ./date: Keine Berechtigung
fr@sushi:/tmp# /lib/ld-linux.so.2 ./date
Sun Jul 29 14:40:32 CEST 2001
```

Viele Tools, die nicht nur ausschließlich von Hackern benutzt werden, versuchen im Verzeichnis */tmp* Dateien anzulegen und diese auszuführen. Mit der Option *noexec* kann man dem Angreifer zumindest das Leben etwas schwerer machen.

3.2.11 Debian Sicherheitsupdates

Sobald eine neue Sicherheitslücke in einem Debian-Paket oder einer Software dieses Pakets bekannt wird, wird von den Paket-Maintainern innerhalb weniger Stunden oder Tage ein Update der betroffenen Pakete bereitgestellt. Das aktualisierte Paket wird unter http://www.debian.org/security/ zur Verfügung gestellt.

Auch für Debian gibt es reichlich Sicherheits-Updates. Um diese sicherheitsrelevanten Patches bei jeder Aktualisierung des Systems automatisch durchzuführen, muss die folgende Zeile in die Datei */etc/apt/sources.list* eingefügt werden:

```
deb http://security.debian.org/debian-security stable/up-
dates \ (security.debian.org/debian-security stable/updates
/)
main contrib non-free
```

In den Ländern, die den Import von kryptographischer Software nicht ausdrücklich verbieten, kann zusätzlich folgende Programmzeile hinzugefügt werden:

```
deb http://security.debian.org/debian-non-US stable/non-US \
(security.debian.org/debian-non-US stable/non-US /)
main contrib non-free
```

Natürlich können auch die entsprechenden *„deb-src“* Zeilen hinzugefügt werden, wenn auch der Zugriff auf die Sourcen gewährleistet sein soll. Danach ist nur noch ein *apt-get update*, gefolgt von einem *apt-get upgrade*, nötig, um das System auf den neuesten Stand zu bringen.

3.2.12 Pluggable Authentication Modules (PAM)

PAM erlauben es dem Systemadministrator auszuwählen, auf welche Weise die verschiedenen Programme eine Authentifizierung durchführen sollen. Hierzu muss jedes Programm an die Verwendung von PAM angepasst sein; dies ist seit Debian 2.2 für die meisten Programme der Fall. Ältere Versionen von Debian benutzen noch keine Authentifizierung über PAM. Für jedes Programm existiert im Verzeichnis */etc/pam.d* eine eigene Konfigurationsdatei.

Mit PAM bietet sich die Möglichkeit, mehrere Authentifizierungsschritte vom Benutzer unbemerkt durchzuführen. Beispielsweise kann eine Authentifizierung sowohl gegen eine Datenbank als auch gegen die Datei /etc/passwd erfolgen.

Über PAM können viele Restriktionen auferlegt werden; genauso gut ist es aber möglich, das System weit zu öffnen und so Sicherheitslücken zu schaffen. Wenn Sie Einstellungen von PAM verändern, sollten Sie also größte Vorsicht walten lassen. Eine typische Konfigurationszeile enthält in der zweiten Spalte ein Kontrollfeld. Dieses sollte auf den Wert „required“ gesetzt werden, so dass bei einem Fehler in einem Modul ein Login verhindert wird.

Password Required

Zuerst sollte die Unterstützung für MD5-verschlüsselte Passwörter aktiviert werden, um zu verhindern, dass ein Passwort leicht von einem Programm über eine Datenbank ermittelt werden kann. Die folgenden Zeilen sollten in allen Dateien in */etc/pam.d/* hinzugefügt werden, die Zugang zu dem Rechnersystem erlauben, beispielsweise *login* und *ssh*.

```
password required pam_cracklib.so retry=3 minlen=12 difok=3
password required pam_unix.so use_authtok nullok md5
```

Der erste Eintrag lädt das Cracklib-PAM-Modul, das strengere Anforderungen an das verwendete Passwort stellt. Passwörter müssen mit diesem Modul mindestens 12 Zeichen haben; bei einer Passwortänderung müssen mindestens drei Zeichen verändert werden. Weiterhin werden nur drei Login-Versuche erlaubt.

Die zweite Zeile benutzt die Standard-Authentifizierung des Unix-Systems mit einer MD5-Verschlüsselung und erlaubt auch leere Passwörter. Die *use_authtok* Option wird benötigt, um das Passwort vom vorhergehenden Modul zu übernehmen.

Anmeldung an Terminals

Um den allgemeinen Zugriff auf einen Rechner so zu beschränken, dass der Benutzer root sich lediglich an einem lokalen System-Terminal anmelden kann, muss die folgende Programmzeile in der Datei /etc/pam.d/login aktiviert werden:

```
auth requisite pam_securetty.so
```

Weiterhin müssen die einzelnen Terminals, von denen dem Benutzer root der Zugriff auf das System gewährt werden soll, in die Datei /etc/security/access.conf eingetragen werden. Um auch die eigentlichen Benutzer des Systems zu beschränken, beispielsweise in der Anzahl der gleichzeitigen Logins auf einen Rechner, muss noch die folgende Zeile aktiviert werden:

```
session required pam_limits.so
```

In der Datei /etc/pam.d/passwd ist nun die erste Zeile zu verändern. Dort muss die Option "md5" eingetragen werden, um mit MD5 verschlüsselte Passwörter zu benutzen. Weiterhin kann die minimale Passwortlänge beispielsweise von 4 auf 6 Zeichen erhöht werden. Ebenso kann eine maximale Länge gesetzt werden, falls dies gewünscht ist. Schlussendlich sollte die Zeile in etwa so aussehen:

```
password required pam_unix.so nullok obscure min=6 max=11 md5
```

PAM-Kommandos

Wenn das Kommando *su* so geschützt werden soll, dass es nur von bestimmten Benutzern ausgeführt werden kann, muss zunächst eine neue Gruppe dem System hinzugefügt werden. Üblich ist es, hierzu die Gruppe „wheel" zu verwenden, da diese üblicherweise noch nicht existiert und es somit unwahrscheinlich ist, dass bereits Dateien zu dieser Gruppe gehören. Dieser Gruppe fügen Sie das Benutzerkonto *root* sowie alle Benutzerkonten hinzu, die das Kommando su ausführen können sollen. In der Datei */etc/pam/su* ist dann folgender Eintrag zu ergänzen:

auth requisite pam_wheel.so group=wheel debug

Somit wird sichergestellt, dass nur die Benutzer, die der Gruppe „wheel" angehören, das Kommando *su* ausführen können. Alle anderen Benutzer bekommen eine entsprechende Meldung, wenn sie versuchen, dieses Kommando auszuführen.

Wenn nur bestimmten Benutzern eine Authentifizierung über PAM erlaubt werden soll, so ist dies relativ einfach über die Dateien zu erreichen, in denen die Benutzer aufgeführt sind, denen der Login erlaubt oder verboten werden soll.

Wenn beispielsweise nur dem Benutzer „fr" der System-Login über *ssh* erlaubt werden soll, so muss dieser in die Datei */etc/sshusers-allowed* eingetragen werden, und folgender Eintrag muss der Datei */etc/pam.d/ssh* hinzugefügt werden:

```
auth required pam_listfile.so item=user sense=allow \
file=/etc/sshusers-allowed onerr=fail
```

Zu guter Letzt sind folgende Einträge der Datei */etc/pam.d/other* hinzuzufügen:

```
auth required pam_securetty.so
auth required pam_unix_auth.so
auth required pam_warn.so
auth required pam_deny.so
account required pam_unix_acct.so
```

```
account required pam_warn.so
account required pam_deny.so
password required pam_unix_passwd.so
password required pam_warn.so
password required pam_deny.so
session required pam_unix_session.so
session required pam_warn.so
session required pam_deny.so
```

Diese Voreinstellungen sind erst einmal eine sinnvolle Vorgabe, denn es werden grundsätzlich erstmal alle PAM-Zugriffe verweigert. Sie sollten auch einen aufmerksamen Blick in die Datei */etc/security/limits.conf* werfen. Hier werden Ressourcen für die Benutzer des Systems festgelegt.

3.2.13 Anpassungen der Datei /etc/inetd.conf

Generell sollten alle nicht benötigten Dienste auf einem System deaktiviert werden. Jeder laufende, nicht unbedingt benötigte Dienst stellt ein potenzielles Risiko dar. Dies betrifft beispielsweise die Dienste *echo*, *charges*, *discard*, *daytime*, *time*, *talk*, *ntalk* sowie die extrem unsicheren „r"-Kommandos wie *rsh*, *rlogin* und *rcp*. Für letztere ist es in jedem Fall besser, die Kommandos *ssh* und *scp* zu benutzen.

Nachdem die nicht benötigten Dienste deaktiviert sind, sollte geprüft werden, ob der Dienst inetd überhaupt noch benötigt wird. Dienste können natürlich auch als Daemon gestartet werden, statt inetd zu benutzen. „Denial of Service«-(DoS-)Angriffe können auch auf den inetd als Ziel ausgeführt werden und so beispielsweise die Systemlast eines Rechners in die Höhe treiben.

Wenn Sie trotzdem nicht auf den Einsatz eines solchen Dienstes verzichten können, so sollten Sie unter Umständen eine Alternative zu inetd einsetzen, die vielfältiger konfiguriert werden kann, beispielsweise den xinetd oder den rlinetd.

Veränderungen an der Datei */etec/inetd.conf* können von Hand vorgenommen werden. Debian bietet aber eine einfach zu benutzende Alternative dazu: Mit dem Programm *update-inetd* können einzelne Dienste verändert werden. Beispiel:

```
/usr/sbin/update-inetd --disable telnet
/etc/init.d/inetd restart
```

Nach jeder Änderung ist der *inetd* noch neu zu starten.

Das Kommando update-ineted

Das Linux-Kommando *update-inetd* kennt noch viele weitere zusätzliche Optionen, beispielsweise auch, um bestimmte unerwünschte Einträge zu löschen:

```
sushi:/home/fr# update-inetd
Usage: update-inetd [OPTION] MODE ARGUMENT
```

```
Options:
--version output version information and exit
--help display this help and exit
--verbose explain what is being done
--debug enables debugging mode
--multi allow multiple removes/disables
--file FILENAME use FILENAME instead of /etc/inetd.conf
--group GROUPNAME add entry to section GROUPNAME
--comment-chars CHARACTERS use CHARACTERS as comment charac-
ters
--pattern PATTERN use PATTERN to select a service

Modes:
--add ENTRY add ENTRY to /etc/inetd.conf
--remove ENTRY remove ENTRY (regular expression)
--enable SERVICE enable SERVICE in /etc/inetd.conf
--disable SERVICE disable SERVICE in /etc/inetd.conf

In order to prevent the shell from changing your ENTRY defi-
nition you have to quote the ENTRY using single or double
quotes. You can use tabs (the tab character or \t) and
spaces to separate the fields of the ENTRY. If you want to
enable/disable more than one SERVICE you can use a comma se-
parated list of services (no whitespace characters allowed).
```

3.2.14 Die Datei /etc/login.defs

In diesem Absatz sollten einige Einstellungen zum Benutzer-Login und zur grundsätzlichen Konfiguration von Debian GNU/Linux vorgenommen werden.

```
FAIL_DELAY              10
```

Diese Variable sollte auf einen höheren Wert gesetzt werden, um „Brute-Force"-Angriffe auf einem Terminal zu erschweren. Wenn ein falsches Passwort eingegeben wird, muss der Benutzer 10 Sekunden warten, bis ein neuer Login-Versuch gestartet werden kann. Dies frisst einiges an Zeit, wenn versucht wird, ein Passwort zu erraten. Diese Einstellung gilt nur, wenn *getty* benutzt wird; bei *mingetty* beispielsweise ist diese Einstellung ohne Wirkung.

```
FAILLOG_ENAB            yes
```

Mit dieser Variablen werden fehlgeschlagene Logins im Logfile verzeichnet. Dies ist wichtig, wenn „Brute-Force"-Angriffe aufgezeichnet werden sollen.

```
LOG_UNKFAIL_ENAB        yes
```

Wenn die Variable *FAILLOG_ENAB* auf *yes* gesetzt wird, so sollte auch diese Variable auf yes gesetzt werden. Diese Einstellung schreibt auch unbekannte Benut-

zernamen bei einem Login-Versuch ins Logfile. Es ist darauf zu achten, dass die entsprechende Logdatei nicht von allen Benutzern gelesen werden kann, da Benutzer häufig anstelle des Benutzernamens das Passwort eingeben. Damit andere Systembenutzer die Logdatei nicht unbedingt lesen können, sind die vergebnen Zugriffsrechte beispielsweise auf *640* zu setzen.

```
SYSLOG_SU_ENAB          yes
```

Diese Einstellung verzeichnet die Benutzung des Kommandos *su* im Syslog.

```
SYSLOG_SG_ENAB          yes
```

Diese Systemeinstellung erfüllt die gleiche Funktion wie die vorhergehende Einstellung, jedoch gilt diese nur für das Kommando *sg*. Mit *sg* ist es möglich ein Linux-Kommandos Auszuführen mit der ID einer anderen Benutzergruppe).

```
MD5_CRYPT_ENAB          yes
```

Wie schon beschrieben, reduzieren MD5-verschlüsselte Passwörter die Gefahr des Erschleichens eines Passwortes durch entsprechende Software. Wenn auf dem System noch „slink“ (Debian 2.1) eingesetzt wird, sollten Sie vor dem Aktivieren dieser Option einen Blick in die Dokumentation werfen. Ansonsten wird diese Einstellung über PAM realisiert.

```
PASS_MAX_LEN            50
```

Wenn MD5-Passwörter in der PAM-Konfiguration vom Admin aktiviert sind, so sollte diese Variable auf den gleichen Wert wie hier aufgeführt gesetzt werden.

3.2.15 Die Datei /etc/ftpusers

Diese Datei enthält eine Liste der Benutzer, die sich nicht per FTP-Protokoll einloggen dürfen. Benutzen Sie diese Datei nur, wenn Sie wirklich sicher sind, dass auf dem System auch tatsächlich ein FTP-Server laufen soll, da per FTP der Benutzername und das Passwort immer im Klartext übertragen werden. Wenn der benutzte FTP-Daemon PAM unterstützt, so können auch dort die Benutzer zugelassen oder ausgeschlossen werden.

3.2.16 Einsatz eines TCP-Wrappers

TCP-Wrapper wurden entwickelt, als noch keine echten Paketfilter verfügbar waren, aber trotzdem eine Kontrolle notwendig wurde. Ein TCP-Wrapper erlaubt oder verbietet einem Rechner oder einer Domäne das Nutzen eines Dienstes. Nähere Informationen finden Sie in der Manpage *hosts_access(5)*.

Im Folgenden sehen Sie vielleicht das kleinste System, um Einbruchsversuche zu registrieren. Auf alle Fälle sollte auf jedem System eine Firewall installiert sein, zusätzlich zu diesem TCP-Wrapper. Dieser kleine Eintrag in die Datei */etc/hosts.deny* schickt bei jedem verweigerten Zugriff auf einen Service eine Admin-Mail.

```
ALL: ALL: spawn ( \
   echo -e "\n\
   TCP Wrappers\: Connection refused\n\
   By\: $(uname -n)\n\
   Process\: %d (pid %p)\n\
   User\: %u\n\
   Host\: %c\n\
   Date\: $(date)\n\
" | /bin/mail -s "Connection to %d blocked" root)
```

Natürlich ist dieses prinzipielle Beispiel nicht absolut perfekt: Bei vielen Netzwerkverbindungen innerhalb einer kurzen Zeit werden natürlich auch entsprechend viele E-Mails gesendet, was wiederum einem DoS-Angriff gleichkommt.

3.2.17 Benutzung von su und sudo

Sollte es einmal notwendig sein, Arbeiten am System als Administrator durchzuführen, so kann das Kommando *su* benutzt werden, um die benötigten Rechte zu erlangen. Versuchen Sie, allen Benutzern klarzumachen, dass Arbeiten als Administrator nur in Ausnahmefällen gestattet sind. In jedem Fall ist ein Login als root zu vermeiden und stattdessen das Kommando *su* zu benutzen. Noch besser ist es jedoch, das Kommando *su* komplett zu entfernen und stattdessen das Kommando sudo zu benutzen, das eine Reihe weiterer Funktionen bietet. Der Befehl *su* ist aber weithin bekannt, da er auch auf vielen anderen Unix-Systemen eingesetzt wird.

sudo erlaubt einem Benutzer, Kommandos unter der ID eines anderen Benutzers auszuführen, gegebenenfalls auch als Administrator. Wenn der Benutzer in der Datei */etc/sudoers* aufgeführt ist und sich authentifiziert hat, können Kommandos ausgeführt werden, die ebenfalls in dieser Datei aufgeführt sind. Verletzungen dieser Regel, wie beispielsweise ein falsches Passwort oder die versuchte Ausführung eines unerlaubten Programms, werden aufgezeichnet und per E-Mail an den Administrator (root) geschickt.

3.2.18 Benutzung von chroot

Der Befehl *chroot* ist eine leistungsfähige Möglichkeit, um ein Programm oder einen Daemon oder einen Benutzer zu beschränken. Man kann sich das wie in einem Gefängnis vorstellen, aus dem ein Ausbruch unmöglich ist (normalerweise … aber einige Leute schaffen es ja doch manchmal ...). Wenn einem Benutzer nicht vollkommen vertraut wird, so kann für diesen eine *chroot*-Umgebung einge-

richtet werden. Dies kann einiges an Festplattenplatz beanspruchen, wenn alle benötigten Binaries und Bibliotheken in diese Umgebung kopiert werden müssen. Aber wenn es dem Benutzer gelingt, Schaden anzurichten, so bleibt dieser auf die durch das Kommando *chroot* definierte Umgebung beschränkt.

Ein gutes Beispiel für eine solche Anwendung ist folgende: Die Authentifizierung erfolgt nicht gegen die Datei */etc/passwd*, sondern gegen LDAP oder/und eine MySQL-Datenbank. Ein verwendeter FTP-Daemon benötigt das Binary und ein paar Bibliotheken. Hier bildet eine *chroot*-Umgebung eine exzellente Verbesserung der Sicherheit, falls eine Sicherheitslücke in diesem FTP-Daemon auftaucht. In diesem Fall ist lediglich die Benutzer-ID des FTP-Daemons betroffen und keine anderen Benutzer des Systems. Natürlich können auch viele andere Dienste von solch einer Umgebung profitieren.

Wichtiger Hinweis: Bisher wird bei keiner bekannten Debian-Linux-Version eine *chroot*-Umgebung für die Systemdienste und Server verwendet.

3.2.19 Kernel-Features

Viele Funktionen des Kernels können während der Laufzeit verändert werden, beispielsweise indem mit dem Kommando *echo* ein Wert in die entsprechende Datei geschrieben wird, oder mit dem Kommando *sysctl*. Mit dem Kommando *sysctl -A* kann angezeigt werden, welche Einstellungen verändert werden können und welche Optionen verfügbar sind. In seltenen Fällen muss etwas verändert werden, aber auf diesem Weg kann die Sicherheit des Systems erhöht werden.

```
/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts = 0
```

Wird die Variable auf den Wert 1 gesetzt, verhält sich das System nach außen wie ein Windows-System, wenn ein Broadcast-ping-Kommando das System erreicht.

```
/proc/sys/net/ipv4/icmp_echo_ignore_all = 0
```

Wenn die ICMP-Pakete auf der vorgeschalteten Firewall nicht explizit geblockt werden sollen, so ist diese Umgebungs-Variable auf den Wert 0 zu setzen.

```
/proc/sys/net/ipv4/tcp_syncookies = 1
```

Diese Option ist ein zweischneidiges Schwert: Einerseits schützt sie gegen „Syn-Flooding-Attacken“, andererseits entspricht dies nicht den RFCs. Diese Option beschäftigt die angreifende Seite ebenso mit „Syn-Floods“, so dass diese gleichermaßen beschäftigt ist. Diese Option kann auch in */etc/network/options* verändert werden, indem die Option *syncookies* auf *yes* gesetzt wird.

```
/proc/sys/net/ipv4/conf/all/log_martians = 1
```

Mit dieser Option-Einstellung werden alle Pakete mit unerlaubten Adressen, beispielsweise wegen eines fehlerhaften Routings, im Netzwerk protokolliert.

3.2.20 Benutzung der svgalib und sichere Übertragung von Dateien

SVGAlib ist eine schöne Einrichtung für Liebhaber der Konsole. In der Vergangenheit sind jedoch immer wieder Sicherheitslücken bekannt geworden. So wurden Sicherheitslücken in *zgv* bekannt, mit denen Administratorrechte erlangt werden konnten. Wenn möglich, sollten Sie auf die Verwendung der SVGAlib verzichten.

Die Übertragung zwischen zwei Rechnern sollte auf keinen Fall mit Programmen wie *ftp* oder *rcp* erfolgen, da diese den Benutzernamen und das Passwort unverschlüsselt übertragen. Als sichere Alternative steht das Programm *scp* zur Verfügung, das im Paket ssh enthalten ist. Hier werden sowohl der Benutzername als auch das Passwort und auch die Daten selbst in verschlüsselter Form übertragen.

3.2.21 Benutzung von Quota

Eine saubere Definition von Benutzerquota ist wichtig, um zu verhindern, dass Benutzer ein komplettes Dateisystem mit Daten füllen können. Es können grundsätzlich zwei verschiedene Quota-Systeme eingesetzt werden: benutzer- oder gruppenorientierte Quota. Dies ist bei der Planung zu berücksichtigen. Einige Punkte sind bei der Benutzung von Quota zu beachten:

- Quota sollten in der Summe so klein gewählt werden, dass nicht der gesamte Festplattenplatz belegt werden kann.
- Quota sollten so groß gewählt werden, dass die Benutzer nicht bei der Arbeit behindert werden. Beispielsweise sollte das Spoolverzeichnis für Mail nicht zu knapp bemessen werden.
- Quota müssen auf allen von Benutzern beschreibbaren Bereichen eingerichtet werden, beispielsweise */home* und */tmp*.

Für jede Partition beziehungsweise jedes Verzeichnis, auf die beziehungsweise das Benutzer Schreibzugriff haben, sollten Quota aktiviert werden. Für diese Bereiche ist ein sinnvoller Wert zu errechnen, der eine Balance zwischen Sicherheit und Benutzbarkeit des Systems schafft.

Doch nun zur Benutzung von Quota: Zunächst müssen Sie prüfen, ob die Quota-Unterstützung im Kernel aktiviert ist. Wenn dies nicht der Fall ist, muss ein neuer Kernel erzeugt werden. Danach ist sicherzustellen, dass das Paket *quota* installiert ist. Quota werden aktiviert, indem in der Datei */etc/fstab* der Eintrag für das entsprechende Dateisystem in der Spalte „Options“ um den Eintrag *usrquota* erweitert wird. Wenn statt Benutzer-Quota Gruppen-Quota benutzt werden sollen, lautet der Eintrag grpquota. Natürlich können auch beide gleichzeitig verwendet werden. Nun müssen im Root-Verzeichnis des Dateisystems leere Dateien *quota.user* und/oder *quota.group* erzeugt werden.

Das Quota-System muss nun neu vom User gestartet werden. Dies geschieht durch die zwei Kommandos */etc/init.d/quota stop* und */etc/init.d/quota start*. Nun können die gewünschten Grenzwerte fürs System vom Anwender gesetzt werden.

Um Quota für einen Benutzer (beispielsweise *fr*) zu setzen, wird das Kommando *edquota -u fr* benutzt. Gruppen-Quota werden mit dem Kommando *edquota -g gruppe* gesetzt. Nun können die unterschiedlichen Grenzwerte für „soft“ und „hard“ sowie für die Inodes gesetzt werden.

3.2.22 Zugriffsrechte von Logdateien und setuid-Check

Einige Logdateien sind nach der Installation nicht perfekt. Zunächst ist es nicht notwendig, dass die Dateien */var/log/lastlog* und */var/log/faillog* von jedem Benutzer gelesen werden können. In der Datei lastlog sind Benutzer verzeichnet, die sich in der letzten Zeit am System angemeldet haben; in der Datei *faillog* finden sich fehlgeschlagene Loginversuche. Bei beiden Dateien sollten die Zugriffsrechte auf *660* verändert werden. Prüfen Sie genau, ob Logdateien mit unnötigen Zugriffsrechten versehen sind. Meist sind Lese- und Schreibrechte für den Administrator und für die Gruppe *adm* oder *root* ausreichend.

setuid-Überprüfungen

Debian wird mit einem täglichen Cronjob installiert, der in */etc/cron.daily/standard* zu finden ist. Der Aufruf von */usr/sbin/checksecurity* fährt eine Überprüfung des Systems auf Änderungen des Flags *setuid* an allen Dateien auf dem System durch. Um diese Überprüfung zu aktivieren, muss die Variable *CHECKSECURITY_DISABLE* in der Datei */etc/checksecurity.conf* auf *FALSE* gesetzt sein. Dies ist auch die Voreinstellung, so dass hier eigentlich keine Änderungen nötig sind.

3.2.23 Kommandos chattr und lsattr

Diese beiden Kommandos sind auf einem *ext2*-Dateisystem sehr sinnvoll. Die Attribute einer Datei können mit *lsattr* angezeigt und mit *chattr* verändert werden. Attribute unterscheiden sich von Zugriffsrechten! Es gibt viele verschiedene Attribute, hier werden nur die sicherheitsrelevanten aufgeführt. Zwei Attribute können nur vom Administrator gesetzt werden.

Zunächst wäre das „a“-Flag zu nennen. Wenn dieses Attribut gesetzt ist, können an die entsprechende Datei nur Daten angehängt (append) werden. Dieses Attribut kann auf einige Dateien in */var/log/* angewendet werden; beachten Sie jedoch, dass einige Dateien von Zeit zu Zeit „rotiert“ werden (unter „rotieren“ versteht man das tägliche Umkopieren und von Logdateien. Dabei werden die Dateien vom Vortag komprimiert. Nach einer bestimmten Zeitspanne, meist eine Woche, werden ältere Dateien gelöscht).

Das zweite wichtige Flag ist „i“, das für „immutable“ steht. Wenn dieses Flag gesetzt wird, kann eine Datei weder verändert noch gelöscht oder umbenannt werden. Auch kann kein Link auf diese Datei erzeugt werden. Wenn Benutzern die Einsicht in Logdateien verwehrt werden soll, so können Sie dieses Flag setzen und die Leserechte entfernen. Dies bietet auch eine etwas höhere Sicherheit gegen Eindringlinge, da diese sich sicher darüber wundern, dass die Datei nicht gelöscht werden kann. Trotzdem sollten Sie sich nicht darauf verlassen, dass ein Eindringling diese Funktion nicht kennt. In jedem Fall ist es ihm zu diesem Zeitpunkt bereits gelungen, in das System einzudringen ...

3.2.24 Integrität des Dateisystems

Sind Sie sicher, dass die auf einem bereits seit Wochen oder Monaten ans Internet angeschlossenen System installierten Programme noch die ursprünglichen sind? Oder kann es sein, dass bereits das Programm */bin/login* durch eine veränderte Variante ersetzt wurde, die einen unbemerkten Login als Administrator erlaubt ...?

Die einzige Methode, ein System gegen solche Veränderungen zu schützen, ist, die installierten Dateien täglich, wöchentlich oder beispielsweise monatlich (je häufiger dieser Test durchgeführt wird, umso weniger Zeit bleibt einem Eindringling, auf dem System zu agieren) mittels einer Checksumme zu dokumentieren und diese mit vorab gespeicherten Werten zu vergleichen.

Pakete, die einen regelmäßigen Check der installierten Pakete ermöglichen, sind: sXid, AIDE (Advanced Intrusion Detection Environment) und Tripwire (die aktuelle Version befindet sich im Bereich non-free, eine der nächsten Versionen wird unter der GPL stehen).

Mit dem mitgelieferten Systempaket *debsums* können alle vorhandenen MD5-Checksummen der installierten Pakete mit den Original-Checksummen der einzelnen Dateien in den Ursprungspaketen der Distribution verglichen werden.

Mittels *debsums -a* können die Checksummen aller Pakete des Systems verglichen werden, wogegen Sie mit *debsums <paketname>* die Checksummen bestimmter Pakete vergleichen. Hierbei ist zu beachten, dass es einem versierten Eindringling durchaus möglich ist, auch diese Kontrolle der Checksummen zu beeinflussen. Die ursprünglichen Checksummen der Pakete liegen in den Dateien */var/lib/dpkg/info/<paketname>.md5sums* und können vom Angreifer auch angepasst werden. Eine höhere Sicherheit bietet das Paket Tripwire.

3.2.25 Die Programme locate und slocate

Um die Sicherheit des Debian-Programms *locate* zu erhöhen, kann als Alternative auch das Programm *slocate* verwendet werden. *slocate* ist eine verbesserte und leistungsfähigere Version von *locate* aus dem Debian GNU/Linux-Projekt.

Wenn *slocate* verwendet wird, werden dem Benutzer nur Dateien angezeigt, auf die dieser Benutzer auch tatsächlich Zugriff hat. Weiterhin können per Konfiguration auch Dateien und Verzeichnisse gezielt ausgeschlossen werden, so dass diese nicht von locate in der Datenbank erfasst werden.

3.2.26 Secure Shell (SSH)

SSH sollte generell für alle Remote-Logins auf einem System eingesetzt werden. Wenn Sie noch *telnetd* einsetzen, so ändern Sie dies jetzt sofort. Heutzutage ist es sehr einfach, den Netzwerkverkehr mitzuschneiden und so an unverschlüsselte Benutzernamen und Passwörter zu gelangen. Die Verwendung von Programmen, die keine verschlüsselte Kommunikation erlauben, verbietet sich somit von selbst. Auch der Einsatz von hochwertigen Netzwerkkomponenten wie Switches erlaubt Angreifern das „Mitlauschen" auf den angeschlossenen Ports! Die meisten Switches schalten bei zu hoher Last einfach das „Switching" ab und arbeiten wie ein normaler Hub! Verlassen Sie sich nie auf diese Komponenten, sondern sorgen Sie selbst für Sicherheit! Das Paket ssh kann mit dem Kommando *apt-get install ssh* schnell und einfach installiert werden.

Nun sollten alle Benutzer angewiesen werden, ausschließlich *ssh* und keinesfalls *telnet* zu benutzen. Deinstallieren Sie telnet nach Möglichkeit. Auch sollte ein Login als Administrator unmöglich gemacht werden. Um Administrator-Rechte zu erlangen, können die Kommandos *su* oder besser *sudo* benutzt werden.

Der ssh-Daemon

Auch die Konfiguration des *ssh*-Daemons kann zur Erhöhung der Systemsicherheit noch wesentlich verbessert werden. In der Datei */etc/ssh/sshd_config* verbietet folgende Zeile einen unerlaubten Login via ssh als System-Administrator:

```
PermitRootLogin No
```

Dies verhindert, dass per Brute-Force-Angriff ein Login als Administrator möglich ist, da kein Login als Administrator erlaubt wird. Es sind nun zwei Login-Vorgänge nötig (zunächst als Benutzer, dieser muss dann Administrator werden):

```
Listen 666
```

Wenn der Port, auf dem der `ssh`-Daemon läuft, verändert wird, so kann dieser einen potenziellen Angreifer auch etwas beschäftigen. Es stehen aber verschiedene Netzwerktools zur Verfügung, mit denen schnell und einfach ermittelt werden kann, auf welchem Port ein Dienst läuft. Verwenden Sie hier nicht zu viel Ehrgeiz.

```
PermitEmptyPasswords no
```

Leere Passwörter sollten ebenfalls verhindert werden.

```
AllowUsers alex bea fr
```

Mit dieser Option wird nur bestimmten Benutzern der Login via *ssh* erlaubt.

```
AllowGroups wheel admin
```

Gleichermaßen wird damit nur bestimmten Gruppen der Zugriff per *ssh* erlaubt.

Benutzer- oder Gruppenzugriff

Um einigen Benutzern oder Gruppen explizit den Zugriff auf das System zu verbieten, stehen die beiden Optionen *DenyUsers* und *DenyGroups* zur Verfügung.

```
PasswordAuthentication no
```

Wird diese Option auf „no“ gesetzt, so ist der Login nur Benutzern gestattet, deren *ssh*-Key der Datei *~/.ssh/authorized_keys* hinzugefügt wurde. Diese Einstellung ist sehr empfehlenswert! Bei Verwendung eines Keys wird das Passwort nicht mehr vom Client zum Server übermittelt. Die Autorisierung wird anhand eines Hash-Wertes geprüft, und der Client erhält lediglich die Freigabe für den Server – oder auch nicht. Weiterhin ist der *ssh*-Daemon so einzustellen, dass ausschließlich das Protokoll der Version 2 verwendet wird. Die Protokollversion 1 ist nach aktuellem Kenntnisstand als angreifbar anzusehen und sollte nicht mehr verwendet werden. Alle diese Optionen beziehen sich auf die Konfigurationsdateien von OpenSSH. Momentan sind drei *ssh*-Pakete im Umlauf: ssh1, ssh2 und OpenSSH, das vom OpenBSD-Team entwickelt wurde. OpenSSH ist eine komplett freie Implementation eines ssh-Daemons, die sowohl ssh1 als auch ssh2 unterstützt. Wenn das Paket „ssh“ installiert wird, so wird das Paket OpenSSH gewählt.

3.2.27 FTP-Server

Wenn auf dem System FTP-Server installiert werden muss, so ist sicherzustellen, dass die Benutzer sich ausschließlich in einer „chroot“-Umgebung bewegen. Diese hält den Benutzer in seinem Home-Verzeichnis gefangen. Mit der Option

```
DefaultRoot ~
```

im globalen Abschnitt der Systemdatei */etc/proftpd.conf* kann dies explizit sichergestellt werden. Danach ist der Server mit dem Kommando */etc/init.d/proftpd restart* von der Veränderung der Systemkonfiguration zu unterrichten.

3.2.28 X-Anwendungen im Netz

Um X-Anwendungen von einem Server aus auf einem Client darzustellen, ist zunächst auf dem Client das Öffnen der Anwendung durch den Server zu erlauben. Vielfach ist zu lesen, dass dies durch das Kommando „*xhost +*“ geschieht. Dies ist

auch prinzipiell nicht falsch, erlaubt jedoch jedem System den Zugriff auf das X-Display. Besser ist es, den Zugriff nur von den gewünschten Systemen aus zu erlauben, indem der entsprechende Rechnername dem Kommando als Option mitgegeben wird, also beispielsweise *xhost +sushi*.

Eine deutlich sicherere Lösung ist es allerdings, die komplette Sitzung über *ssh* – und damit verschlüsselt – zu tunneln. Dies erfolgt automatisch, wenn eine *ssh*-Verbindung zu einem System aufgebaut wird. Soll diese Funktion abgeschaltet werden, so ist die Option *X11Forwarding* in der *ssh*-Konfiguration anzupassen. In Zeiten von *ssh* sollte auf die Verwendung von *xhost* komplett verzichtet werden.

Wenn keinerlei Zugriff auf den X-Server von anderen Systemen im Netz erlaubt werden soll, so ist es das Sicherste, dies bereits beim Start von X zu verhindern, indem der TCP-Port 6000 deaktiviert wird. Wenn X über das Kommando *startx* gestartet wird, so kann dies mit *startx -- -nolisten tcp* geschehen.

3.2.29 Display-Manager

Wenn der Display-Manager (das Programm, das einen grafischen Login bereitstellt, beispielsweise XDM, KDM oder GDM) nur auf dem lokalen System benötigt wird, so ist sicherzustellen, dass XDMCP (X Display Manager Control Protocol) deaktiviert ist. Wenn das Programm *xdm* benutzt wird, kann dies durch

```
DisplayManager.requestPort:     0
```

in der Datei */etc/X11/xdm/xdm-config* geschehen. Die XDMCP-Unterstützung ist bei der Grundinstallation aller Display Manager unter Debian deaktiviert.

3.2.30 E-Mail

Das Lesen beziehungsweise Empfangen von E-Mail mittels POP3 ist das am häufigsten eingesetzte Protokoll ohne Verschlüsselung. Unabhängig davon, ob POP3 oder IMAP als Protokoll verwendet wird – beide benutzen Benutzernamen und Passwörter im Klartext, und auch die Daten werden unverschlüsselt übertragen. Als Alternative kann auch hier *ssh* verwendet werden, falls ein Shell-Account auf dem Mail-Server vorhanden ist.

Mittels des *fetchmail*-Befehls kann über ssh eine sichere verschlüsselte Verbindung aufgebaut werden; hierzu ein entsprtechendes Beispiel mit *~/.fetchmailrc*:

```
poll my-imap-mailserver.org via "localhost"
with proto IMAP port 1236
user "ref" there with password „hackme“ is alex here war-
nings 3600
folders
.Mail/debian
preconnect ,ssh -f -P -C -L 1236:my-imap-mailserver.org:143
```

```
-l ref
my-imap-mailserver.org sleep 15 < /dev/null > /dev/null‘
```

Die wichtigste Zeile ist der “preconnect“-Eintrag. Dieser startet eine *ssh*-Session und installiert einen Tunnel, der automatisch die Verbindungen zum IMAP-Server auf Port 1236 weiterreicht, verschlüsselt. Dies nur als ein Beispiel, normalerweise sind einfachere Konfigurationen ausreichend. Alternativ kann *fetchmail* auch mit SSL benutzt werden.

Wenn verschlüsselte IMAP- und POP3-Server zur Verfügung gestellt werden sollen, so ist das Paket *stunnel* zu installieren. Die Daemons müssen dann über *stunnel -p /etc/ssl/certs/stunnel.pem -d pop3s -l /usr/sbin/popd* gestartet werden, wobei *-l* den gewünschten Daemon und *-d* den Port beschreibt. Die Option *-p* setzt das SSLZertifikat. Mittlerweile sind auch POP- und IMAP-Server verfügbar, die über Verschlüsselungsfunktionen mittels SSL verfügen. Als Server-Programm für das POP-Protokoll wäre hier *apop* zu nennen.

3.2.31 Loghost – ein Server für Logdateien

Ein „Loghost“ ist ein zentraler Rechner, auf dem Daten aus dem Syslog-Daemon verschiedener Rechner gespeichert werden. Wenn ein Eindringling ein System geknackt hat, so ist es ihm unmöglich, die Spuren aus den Logdateien zu entfernen, außer er knackt auch noch den Loghost. Somit sollte speziell ein solcher Loghost gut abgesichert sein. Um ein System in einen Loghost umzuwandeln, muss lediglich der *syslog*-Daemon mit der Option *-r* gestartet werden. Natürlich muss aber auch auf allen Rechnern, die nun die Daten auf diesem Loghost abliefern sollen, eine Anpassung erfolgen. Auf diesen Systemen sind in der Datei */etc/syslog.conf* Einträge in der folgenden Form hinzuzufügen:

```
<facility>.<level> @<loghost>
```

Das Feld <facility> kann dabei einen Werte *authpriv*, *cron*, *daemon*, *kern*, *lpr*, *mail*, *news*, *syslog*, *user*, *uucp* oder *local1* bis *local7* annehmen. Als <*level*> kann *alert*, *crit*, *err*, *warning*, *notice* oder *info* angegeben werden. Hinter dem Sinderzeichen „*@*“ ist der Hostname des Loghosts zwingend anzugeben.

Wenn generell alle relevanten Rechnereinträge auf dem entfernten System mit protokolliert werden sollen, so führt folgende Befehls-Zeile zum Erfolg:

```
*.*    @loghost
```

Im Idealfall wird man die Logdateien sowohl auf dem lokalen System als auch auf dem Loghost speichern, um durch Vergleichen der Dateien schneller zu einem Ergebnis zu kommen. Weitere Informationen finden Sie in den Manpages zu *syslog(3)*, *syslogd(8)* und *syslog.conf(5)*.

3.2.32 BIND und Snort

Auf einem unveränderten System läuft der Nameserver BIND nach der Installation mit den Rechten des Benutzers und der Gruppe „root“. BIND kann leicht umkonfiguriert werden, so dass der Dienst unter einem anderen Benutzerkonto läuft. Leider kann er dann nicht mehr automatisch neue Netzwerkgeräte erkennen, die während des laufenden Betriebs hinzugefügt wurden, beispielsweise eine PCMCIA-Netzwerkkarte in einem Notebook oder auch virtuelle Netzwerk-Devices.

In der Datei *README.Debian* des Nameservers finden Sie weitere Informationen darüber, wie Sie BIND unter einem anderen Benutzerkonto zum Laufen bringen können. Wenn möglich, sollten Sie unbedingt darauf verzichten, BIND mit sicherheitssensitiven Administratorrechten zu benutzen.

Um BIND mit einer anderen Benutzer-ID zu starten, muss zunächst ein neuer Benutzer und eine entsprechende Systemgruppe angelegt werden. Es kann beispielsweise als Benutzername und Gruppe der Name „named“ verwendet werden.

Hierzu sind folgende Kommandos notwendig:

```
addgroup named
adduser --system --ingroup named named
```

Nun muss in der Datei */etc/init.d/bind* der Eintrag

```
start-stop-daemon --start
```

geändert werden in

```
start-stop-daemon --start --quiet --exec /usr/sbin/named --
-g named -u named
```

Natürlich ist BIND im Anschluss nun noch mit */etc/init.d/bind stop* und */etc/init.d/bind start* neu zu starten. Dabei sollten in der Datei Syslog (*/var/log/syslog*) in etwa folgende Systemeinträge in Textform auftauchen:

```
Jul 8 23:21:01 sushi named[12432]: group = named
Jul 8 23:21:01 sushi named[12432]: user = named
```

Damit ist die Umstellung im Großen und Ganzen abgeschlossen. Idealerweise kann BIND nun noch in einer sicheren „chroot“-Umgebung betrieben werden.

Snort

Snort ist ein flexibler Packet-Sniffer, der verschiedenste Angriffe ermitteln kann. Hierzu gehören Buffer-Overflows, CGI-Angriffe, SMB-Angriffe und vieles mehr. Snort kann Alarmierungen in Echtzeit durchführen. Dieses Programm sollte auf jedem Router installiert sein, um jederzeit das Netzwerk zu überwachen. Die Installation erfolgt mit einem *apt-get install snort*; beantworten Sie die Fragen, und werfen Sie dann einen Blick auf die Logdateien.

3.2.33 Debian-Sicherheits-Updates

Unmittelbar nach jeder neuen Debian-GNU-Installation, beispielsweise von CD, sollten die neuesten verfügbaren Security-Updates installiert werden. Durch die notwendigen Vorlaufzeiten bei der Produktion von CDs sind diese natürlich nicht immer auf dem neuesten Stand. Natürlich ist es nicht ausreichend, ein solches Update einmalig auszuführen, vielmehr müssen diese Updates in regelmäßigen Abständen durchgeführt werden. Dies verhindert, dass Software mit bekannten Sicherheitslücken über längere Zeit im laufenden Betrieb verwendet wird.

3.2.34 Austausch von Software

Zunächst sollten alle Netzwerkdienste, deren Passwörter im Klartext übertragen werden, deaktiviert oder gegen Versionen mit verschlüsselter Kommunikation getauscht werden. Dies betrifft Dienste wie FTP, Telnet, NIS, RPC und so weiter.

Auch sollten Sie auf die Verwendung von NIS (Network Information Service) verzichten. Bei einer fehlerhaften Konfiguration kann es leicht zu Sicherheitslücken kommen. Zusätzlich sollten Sie RPC deaktivieren, sofern es möglich ist. Natürlich wird gerade NFS häufig verwendet und stellt in vielen Netzen einen wichtigen Basisdienst dar. Hier gilt es, einen Kompromiss zwischen Sicherheit und Benutzbarkeit der Netzwerkdienste zu finden. Viele DDoS-(Distributed Denial of Service-)Angriffe benutzen RPC-Sicherheitslücken, um Systeme in so genannte „Agents“ oder „Handler“ umzuwandeln.

Das Deaktivieren des Portmappers ist relativ einfach. Wie für jede Lösung gibt es auch hier verschiedene Wege. Auf einem Debian-System ist der einfachste Weg sicherlich ein *update-rc.d portmap remove*. Dieses Kommando löscht jeden symbolischen Link auf den Portmapper in */etc/rc${runlevel}.d/*. Dies kann natürlich auch auf herkömmlichem Wege von Hand erledigt werden. Eine weitere, nicht ganz elegante Möglichkeit ist es, die Zugriffsrechte so zu ändern, dass das Script nicht mehr ausführbar ist. Dazu verwenden Sie *chmod 644 /etc/init.d/portmap*. Dies würde jedoch zu einer Fehlermeldung beim Start des Systems führen.

Natürlich ergibt es nur wenig Sinn, lediglich einen Teil der Dienste von unverschlüsselter auf verschlüsselte Kommunikation umzustellen; hier sollte der Systemadministrator konsequent durchgreifen. Generell sollten die Dienste *ftp*, *telnet*, *pop*, *imap* und *http* entfernt und durch die entsprechenden Dienste mit verschlüsselter Kommunikation (*ftp-ssl*, *telnet-ssl*, *pop-ssl*, *https*) ersetzt werden.

3.2.35 Kernel-Patches

Im Internet sind ein große Anzahl von Kernel-Patches verfügbar, die nicht Bestandteil des Standard-Linux-Kernels sind, dessen Sicherheit aber verbessern. Vor dem Einsatz solcher Programme ist im Einzelfall zu prüfen, ob der gewünschte

Patch nicht schon in den benutzten Kernel eingeflossen ist. Auch erhebt die folgende Auflistung natürlich keinerlei Anspruch auf Vollständigkeit und Funktion.

OpenWall Patch von „Solar Designer". Eine Sammlung von Patches, die etwa Links beschränken, FIFOs in */tmp/* unterbinden, das */proc*-Dateisystem schützen, die Behandlung von Datei-Deskriptoren ändern und einiges andere verändern. Momentan werden Kernel der Serien 2.0, 2.2 und 2.4 unterstützt. Detaillierte Informationen finden Sie auf der Homepage www.openwall.com/linux.

LIDS – Linux intrusion detection system von Huagang Xie und Philippe Biondi. Dieser Patch vereinfacht die Sicherung eines Linux-Systems. Jeder Prozess kann beschränkt werden, indem Lese- und Schreibberechtigungen auf Dateien vergeben werden können. Weiterhin können je Prozess „Capabilities" gesetzt werden. Dieser Patch findet sich unter www.lids.org.

POSIX Access Control Lists (ACLs) für Linux. Der Patch erweitert den Kernel um Access Control Lists (ACLs), eine Methode, die es gestattet, den Zugriff auf Dateien detaillierter als üblich zu beschränken. URL: http://acl.bestbits.at.

Linux trustees. Mit dem Patch wird ein erweitertes System mit Zugriffsrechten zum Kernel hinzugefügt. Alle Objekte werden im Kernel-Speicher gehalten, so dass ein schneller Zugriff möglich ist. www.braysystems.com/linux/trustees.html.

International kernel patch. Dieser Patch implementiert kryptographische Dateisysteme im Kernel. Es sind in einigen expliziten Ländern die entsprechenden Gesetze dringend zu beachten. Die entsprechende Homepage: www.kerneli.org.

SubDomain. Mit diesem Patch kann eine noch sicherere chroot-Umgebung aufgesetzt werden. Die für die Umgebung benötigten Dateien können einzeln angegeben werden und müssen nicht mit einkompiliert werden. Homepage: http://www.seifried.org/security/products.

UserIPAcct. Der Patch bezieht sich nicht direkt auf die Sicherheit eines Systems, erhöht aber die Kontrolle über die unberechenbaren Benutzer. So können Quota, bezogen auf den Benutzer, für den Netzwerkverkehr vergeben werden. Statistiken sind auch verfügbar. Homepage: http://ramses.smeyers.be/homepage/useripacct.

FreeS/WAN. Um IPSec zusammen mit dem Linux-Kernel verwenden zu können, wird dieser Patch benötigt. Hiermit können VPNs (Virtual Private Networks) leicht aufgesetzt werden, zur Not auch mit Windows-Rechnern auf der Gegenseite. IPSec ist der für VPNs eingebürgerte Standard. Homepage: http://www.freeswan.org.

3.2.36 Cruft

Eine wichtige Aufgabe des Systemadministrators ist die regelmäßige Überwachung aller Dateien im System. Ein Eindringling kann es nicht nur auf den Diebstahl von Daten abgesehen haben, auch das Verändern von Systemdateien (beispielsweise um neue Benutzer anzulegen) oder von Programmdateien (Austausch von Binaries durch veränderte Versionen) kann ein Ziel sein. Das Auffinden dieser

Veränderungen ist nur möglich, wenn der Stand vor der Veränderung bekannt ist. Debian unterstützt durch die ausgefeilte Paketsystemtechnik die Überprüfung der installierten Dateien. Als erster Einstieg kann das Systemprogramm *cruft* dienen.

cruft untersucht das komplette Dateisystem nach Dateien, die eigentlich nicht vorhanden sein sollten, beziehungsweise nach Dateien, die sich nicht mehr im Dateisystem finden lassen. Hierzu wird im Wesentlichen auf die Informationen aus den Dateien im Verzeichnis */var/lib/dpkg/info/* zugegriffen. *cruft* überwacht aber auch darüber hinausgehende Informationen wie beispielsweise die „alternatives"-Informationen, die *lost+found*-Verzeichnisse in einem *ext2*-Dateisystem und auch die Heimatverzeichnisse der Benutzer.

3.2.37 Weitere Möglichkeiten

Im Folgenden finden Sie einige Gedanken dazu, wie das bisher Gesagte weiterhin umgesetzt werden kann. Das PAM-System ist durch den modularen Aufbau in der Lage, die verschiedensten Medien zur Authentifizierung zu nutzen. Wie wäre es mit einem Scanner für Fingerabdrücke oder einem Iris-Scanner?

Alle bisherigen Logdaten wurden auch in Dateien geschrieben. Diese können von einem Angreifer natürlich verändert oder gelöscht werden, auch wenn diese auf anderen Rechnern gespeichert werden. Logfiles, die auf einem Drucker mit Endlospapier ausgegeben werden, können nicht gelöscht werden!

Um das Löschen oder das Verändern von Dateien zu verhindern, kann ein komplettes System einmalig konfiguriert werden und dann auf eine bootfähige CD-ROM geschrieben werden. Natürlich sind so noch Angriffe auf das System möglich; es können aber keine Daten verändert oder zusätzliche Programme installiert werden. Für ein Firewall-System ist dies beispielsweise eine sinnvolle Möglichkeit, das System zu schützen.

Wenn möglich sollten alle Kernel-Treiber nicht als Module übersetzt werden. Dann kann die Möglichkeit, Kernel-Module zu laden, komplett deaktiviert werden. So können viele Angriffe abgewehrt werden. Auch hier gilt: Nicht benutzte Funktionen sind abzuschalten.

3.2.38 Maßnahmen nach einem Einbruch ...

Nach einem potentiellen Einbruch ins System gibt es nicht viel zu tun. Das System sollte man sofort vom Netz nehmen und komplett neu zu installieren. Einfach, nicht wahr? Natürlich gilt es herauszufinden, wie der Eindringling in das System eingedrungen ist. Dies geschieht in einer abgeschotteten und sicheren Umgebung, also ohne Netzzugang für das betroffene „infizierte" System. Es sind zur späteren weiteren Analyse und Ursachenforschung alle Daten auf einem geeigneten Medium (zum Beispiel externe Festplatte) zu sichern.

Gegebenenfalls ist eine Meldung an ein CERT (Computer Emergency Response Team, in Deutschland beispielsweise das DFN-CERT http://www.cert.dfn.de) zu erstellen und dort der Einbruch zu melden. Ist eine Strafverfolgung des Einbruchs vorgesehen oder geplant, so sollten Sie gegebenenfalls auf professionelle Unterstützung zurückgreifen. Weiterhin sind auf dem neuen System alle notwendigen, vorab beschriebenen Sicherheitsvorkehrungen zu treffen.

3.2.39 Erkennen von Rootkits

Nach einem Einbruch auf einem System, beispielsweise durch ein über das Netzwerk gesnifftes Passwort, werden häufig so genannte „Rootkits“ installiert, die dem Angreifer einen Zugang mit Rechten des Administrators (root) erlauben.

Es ist dabei über eine offene Sicherheitslücke, die dem potentiellen Angreifer zunächst lediglich normale Systembenutzerrechte erlaubt, möglich, mittels bekannter Lücken weitere unerwünschte Zugriffsrechte auf den Rechner zu erlangen.

Ein Rootkit wird dabei, wie der Name schon sagt, als „Bausatz“ in Form von Scripts geliefert. Rootkits sind in den verschiedensten Varianten im Internet verfügbar. Der Angreifer muss nicht zwingend über weit reichende Systemkenntnisse verfügen, ein erschlichener Benutzer-Account ist oft ausreichend, um ein Rootkit zu installieren. Angreifer, die solche Rootkits einsetzen, werden daher aufgrund des fehlenden Know-hows auch als „Script-Kiddies“ bezeichnet.

Rootkits haben dabei die (unangenehme) Eigenschaft, viele Arbeitsschritte bei einem Einbruch in ein System zu automatisieren. Es werden dabei zunächst Programme installiert und ausgetauscht, um Aktivitäten auf dem System zu verbergen. Dabei ist es beispielsweise üblich, zunächst */bin/login* gegen eine modifizierte Variante auszutauschen. Die neue Version erlaubt Logins eines bestimmten Benutzers ohne oder mit einem bekannten Passwort. Natürlich erscheinen diese Logins in keinem Logfile. Weiterhin werden Programme, die Aufschlüsse über die Aktivität von Benutzern erlauben, durch veränderte Versionen ersetzt. Dies betrifft meist Programme wie *ls* (Anzeigen von Dateien und Zugriffsrechten) oder auch *ps* (Anzeigen von Prozessen eines Benutzers). Mit diesen neuen Programmen werden Aktivitäten des Angreifers verschleiert oder verborgen.

3.2.40 Rootkit-Tools

Um ein Rootkit zu erkennen, können Sie das Paket *chkrootkit* (Check Rootkit) verwenden. Dieses kann ab der Debian-Version 3.1 direkt via APT installiert werden. Der Aufruf dieses Programms erfolgt wie üblich auf der Kommandozeile, es kann dabei die Option *-q* angegeben werden, um die Informationen über die durchgeführten Tests zu unterdrücken. Leider neigt *chkrootkit* dazu, mitunter Alarm zu schlagen, auch wenn kein Rootkit installiert ist. Bekannt ist dies bei Netzwerkinterfaces, die im Promiscous-Modus laufen (wenn beispielsweise

tcpdump eingesetzt wird). Bekannt ist dieses Fehlverhalten auch bei Kerneln mit NPTL-Patch (ab Kernel 2.6 immer enthalten); dabei wird ein „LKM-Trojaner“ gemeldet. Weiterhin werden solche falsch-positiven Ergebnisse auch auf sehr langsamen Rechnern gemeldet.

Suckit Detection Tool

Das für Debian GNU/Linux mitgelieferte Programmpaket *skdetect* ist eine auf das „Suckit“-Rootkit spezialisierte Software. Einige auf Debian abgestimmte Tests wurden hier genauer implementiert, die Erkennung ist aber nicht so umfassend.

3.2.41 Fazit

Grundsätzlich enthält jedes System nach der Neuinstallation Sicherheitslücken. Je nach Einsatzgebiet des Rechners müssen diese Schwachstellen erst beseitigt werden. Debian GNU/Linux bietet umfangreiche Möglichkeiten, das System vor unbefugten Zugriffen abzuschotten. Allerdings reicht es nicht aus nur Sicherheits-Updates aufzuspielen. Der Anwender selbst kann und muss aktiv sein System „härten“. Über Sicherheitsrisiken unter Debian GNU/Linux kann sich der Anwender im „Securing Debian HOWTO“ bereits im Vorfeld informieren. Auch vor, während und nach der Installation des Debian-Betriebssystems muss der User auf einige Grundlegende Dinge achten. Das beginnt bei den BIOS-Einstellungen geht über Absicherung des Bootloaders und Aufspielen von Sicherheits-Patches bis hin zu Anpassungen von Diensten und sicherheitsrelevanten Dateien. (hal)

Weiterführende Infos

Die Artikelserie basiert auf dem Kapitel 14 des Standardwerks „Debian GNU/Linux Anwenderhandbuch für Einsteiger, Umsteiger und Fortgeschrittene“ von Frank Ronneburg aus dem Verlag Addison-Wesley. Sie können dieses über 750 Seiten starke Buch auch in unserem Buchshop unter dem Webcode „buchshop“ bestellen oder als eBook herunterladen.

tecCHANNEL-Links zum Thema	Webcode	Compact
Systemsicherheit mit Debian GNU/Linux	433931	S.170
Komplette Überwachung mit Zabbix	430811	–
Linux-Installation mit apt	430675	–

Glossar

➥
Fortsetzung des Listings der vorangegangenen Zeile.

CGI

Common Gateway Interface. Definierte Schnittstelle, über die der Webserver externe Programme aufrufen und deren Ergebnisse als Webseiten zur Verfügung stellen kann.

Daemon

Ein Daemon lässt sich mit einem Dienst unter Windows NT vergleichen. Er stellt beispielsweise einen FTP- oder HTTP-Server zur Verfügung.

DHCP

Dynamic Host Configuration Protocol. Bei DHCP bezieht ein Arbeitsrechner seine Konfiguration des IP-Netzwerks von einem Server.

DMZ

Entmilitarisierte Zone, demilitarized zone: Dabei befinden sich Bastion-Host, Informations-Server, Modem-Pools sowie andere Server im DMZ-Netz.

DNS

Domain Name System (oder Service). Internet-Dienst, der Domain-Namen wie www.ibm.de in die zugehörigen IP-Adressen umsetzt.

DoS

Denial of Service. Hacker-Angriff auf einen Rechner, der den angegriffenen Computer lahm legt, so dass er auf Anfragen nicht mehr reagieren kann.

DSL

Digital Subscriber Line. Die Standleitung ins Internet für kleine Firmen und Privatpersonen. DSL arbeitet mit denselben Kupferkabeln wie analoge Telefone und ISDN-Anschlüsse.

FAQs

Frequently Asked Questions. Eine Liste häufig gestellter Fragen mit den dazugehörigen Antworten. FAQs werden von Herstellern und Anwendern zu zahlreichen Themen angeboten.

Firewall

Software zur Sicherung des LAN vor Angriffen aus dem Internet.

https

Protokollkennzeichner für über SSL gesicherte http-Verbindungen.

IANA

Internet Assigned Numbers Authority. Zeichnet für die Administration des Domain Name System (DNS) verantwortlich. Regelt über regionale Registrare die Vergabe von IP-Adressen und Top Level Domains (TLDs).

ICMP

Internet Control Message Protocol. TCP/IP-Protokoll zum Austausch von Fehler- und Statusmeldungen.

LDAP

Lightweight Directory Access Protocol. Standardisiertes Netzwerkprotokoll zum Zugriff auf Verzeichnisdienste, über die sich Ressourcen wie etwa E-Mail-Adressen finden lassen.

Masquerading / NAT

Network Address Translation. Bei NAT handelt es sich um ein Verfahren zur Abschottung des LAN gegenüber dem Internet. Dabei wird zum Internet hin immer nur die Adresse des Gateways gemeldet.

MD5

Beim dem Message-Digest-Algorithmus Version 5 handelt es sich um einen Verschlüsselungsalgorithmus, der vorwiegend zur Erzeugung digitaler Signaturen verwendet wird.

NFS

Network File System. Spezielles Dateisystem, das in Unix-Umgebungen den Zugriff auf entfernte Verzeichnisse und Dateien ermöglicht.

NIS

Network Information Services. Früher als Yellow Pages (YP) bezeichnet. Dient der Verteilung von wichtigen Daten (Passwörter, Adressen, Schlüssel-Codes) vom Server an den Client.

NOS

Network Operating System, Netzwerkbetriebssystem. Allgemeine Bezeichnung für Betriebssystem, das für den Server-Einsatz vorgesehen ist, wie zum Beispiel Novell Netware oder Windows NT Server.

PAM

Pluggable Authentication Modules. Bezeichnet mehrere Bibliotheken, die für Unix-Anwendungen gemeinsame Methoden zur Benutzerauthentifizierung zur Verfügung stellen. Neben der eigentlichen Authentifizierung stellen PAMs auch Methoden zur Behandlung von Benutzerkonten und Sitzungsdaten zur Verfügung.

PAP

Password Authentication Protocol. Bei PAP authentifiziert sich ein Einwahl-Client per Benutzernamen und Passwort beim Server.

POP / POP3

Post Office Protocol. Eines von zwei Standardprotokollen zur Zustellung von E-Mails an einen Mail User Agent. Alle gängigen E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server.

Port

Ein TCP-Port dient als Kommunikationskanal für den Zugriff auf einen Internet-Rechner über das TCP/IP-Protokoll, ähnlich den Nebenstellen eines Telefonanschlusses.

Index

A

Absicherung des Bootloaders 174
abstract 104
ACL 151, 154
Active Directory 117
Active Directory-Datenbank defragmentieren 146
admin users 156
Adressierung 27
Adressklassen 37
Agents, Directory Service 94
Aliasnamen 78
ATM 61
Ausfall einer WAN-Leitung 134
Ausfall eines Domänencontrollers 119
Authentifizierung 109
auxiliary 104

B

Backslash 153
BIND 70, 191
Bind, SASL 110
block device 155
BNF 102
Broadcast-Datenverkehr 57
Broadcast-Domäne 15, 51
Brückenkopfserver auswählen 132

C

Cachen von Mitgliedschaften 120
Canonical Name 78
character device 155
chattr 185
chroot 182
CRC-Prüfsumme 15
Cruft 193

D

Debian GNU/Linux 170
Debian Sicherheitsupdates 176
Distanzvektor 33
DIT 93
DNS 70
DNS-Lookup 81
DNS-Server-Ausfall 117
DNS-Updates 87
DNS-Zone 118
DNSsec 87
Domain Name Pointer 79
Domain Name Service 70, 71
Domänen-Naming-Master 125
DSA 94
DSRM-Passwort 138
Dynamische VLANs 52

E

EA 154
erweiterten Attribute 154
EXTERNAL 111

F

Festplattenpartitionen 172
Flexible Single Master Operations 124
force group 157
force user 157
Forwarder 83
FQDN 78
Frame-Tagging 59
Freigabedefinitionen 156
FSMO 124
FTP_Server 188
ftpusers 181

G

Global Catalog 119
GSSAPI 111
guest ok 157

I

Identifier, Unique Object 93
inetd.conf 179
Infrastrukturmaster 125, 127
Inter-Switch Link 60
invalid users 157
IP-Paket 17
IP-Subnetz 56
IPv6-Adressen 78
IPX 12
ISTG auswählen 133

K

KERBEROS_V4 110
Kernel-Features 183
Kernel-Patches 192
Kollisionsdomäne 15

L

LANE 61
LAN Emulation 61
LDAP 90
LDAP-Anfragen 119
LDAP-Schema 93
LDAP-Tools 115
LDAPv3 90
LDIF 104
Lightweight Directory Access Protocol 90
locate 186
Loghost 190
login.defs 180
lsattr 185

M

MAC-Adresse 12, 56
Mail-Exchanger 80
Mailinglisten 174
Masterfile-Format 75
MD5, DIGEST 111
Metrik 20, 31
MMC 161
Mounten von Dateisystemen 175

N

Name, Distinguished 95
Name, Relative Distinguished 93
Name-Service 77
named 70, 84
Namensraum 153
Nameserver 70
Netzlaufwerksdefinitionen 152
Netzlaufwerkskontroll-Listen 152
Ntbackup 135
Ntdsutil 121, 128
NTFS 152

O

Objekt-ID 98
OID 93, 98
only user 157
OpenLDAP 93

P

PAM 177
Passwörter und aktivierte Dienste 173
PDC-Emulator 125
pipe device 155
PLAIN 110
Pluggable Authentication Modules 177
Primary Nameserver 73
Private Key 87
Protokolle 10
Public-Key-Infrastruktur 88

Q

Quota 184

R

RDN 93
read list 157
Reverse-Lookup 77
RID-Master 125
Rollenmaster entziehen 130
root 153
Root-Nameserver 71
Rootkit-Tools 195
Rootkits 195
Routing 10
Routing-Algorithmen 30
Routing-Protokolle 19, 25
Routing-Tabellen 29

S

Samba 151
Schema 97
Schemamaster 125
Schicht-3-Gerät 14
Secondary Nameserver 82
Secure Shell 187
Securing Debian HOWTO 171
Service, Directory 90
setuid 185
Slash 153
Slave-Nameserver 83
Slave-Server 83
slocate 186
Snort 191
SOA 76
SOA-Eintrag 118
SSH 187
Start Of Authority 76

Statische VLANs 51
structural 103
su 182
Subnetzmasken 10
Suckit Detection Tool 196
sudo 182
svgalib 184
Systemsicherheit 170
Systemstatus-Backup 136

T

task-harden 170
TCP-Wrappers 181
Tree, Directory Information 93, 95

U

UNIX-Dateisystem 152
UNIX-Domain-Socket 155
username 157

V

V5, Kerberos 111
valid users 157
verbindungslos 13
Verknüpfungen 154
Verlust zentraler Replikations-
komponenten 131
Verzeichnisdienst 90
Virtual LAN 10, 48
VLAN 48
VLAN-Frames 59
VLAN-Topologien 48
VoIP-Installationen 48, 70, 117, 151, 170

W

write list 157

X

X-Anwendungen 188
X.500 90
X.509 111

Z

Zugriffskontroll-Listen 151
Zugriffskontrollen 156, 160
Zugriffssteuerung 107